IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 June 2024, accepted 22 July 2024, date of publication 25 July 2024, date of current version 6 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3433404

RESEARCH ARTICLE

Research on Quantitative Prioritization Techniques for Selecting Optimal Security Measures

JANG JISOO[1], SUBONG JUNG[2], MYUNGKIL AHN[3], DONGHWA KIM[3], JAEPIL YOUN[4], AND DONGKYOO SHIN[1,5,6]

[1]Department of Computer Engineering, Sejong University, Seoul 05006, South Korea
[2]Defense Future Technology Laboratory, LIG System, Seoul 03130, Republic of Korea
[3]Cyber Technology Center, Agency for Defense Development, Seoul 05771, Republic of Korea
[4]Department of Joint Education, Joint Forces Military University (JFMU), Nonsan-si, Chungcheongnam-do 33021, Republic of Korea
[5]Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, South Korea
[6]Cyber Warfare Research Institute, Sejong University, Seoul 05006, South Korea

Corresponding author: Dongkyoo Shin (shindk@sejong.ac.kr)

This work was supported by the Defense Acquisition Program Administration and the Agency for Defense Development Project Name: Cyber Warfare Mission Impact Analysis Tool Development Prototype under Project UC220012XD.

ABSTRACT Many organizations and researchers, such as NIST, FIRST, MITRE, etc. in the United States, are conducting various cybersecurity research to counter the evolving cyber threats. Research on improving the security level of systems and networks by checking the network environment is one of the main areas of continuous research. To choose the right security countermeasures, you need to ensure that the defense techniques they contain are appropriate for your systems and networks. However, how to determine this is a difficult and complex issue, and as cyber threats evolve, how to determine this will need to evolve with them. To address these issues, this study quantitatively designed six metrics for defense technologies based on system and network environments and used them to conduct experiments on the entire network, as well as experiments on security countermeasures after a cyber-threat has caused damage in a virtual network environment. The proposed method was able to cover a large number of vulnerabilities relative to the number of mitigation techniques applied, and the prioritized list of mitigation candidates allowed us to select the appropriate list of defense techniques for the network. This research can be developed into an automated technology that collects vulnerabilities for the entire system of the network environment to be applied in the future, measures the defense level, prioritizes the complementary defense technologies, and lists them as defenses.

INDEX TERMS Cybersecurity, cyberspace, cyber warfare.

I. INTRODUCTION

Traditionally, anti-malware and anti-virus tools have been the primary tools and techniques for preventing cybercrime [1]. However, the complexity and diversity of current cybercrime has surpassed the capabilities of these traditional security tools. As a result, cybersecurity researchers believe that the development of new and effective security systems to counter threats is an urgent task [2]. Furthermore, one of the reasons for the in-crease in cyber threats is that cybersecurity policies need to be understood in the context of the ever-changing cybersecurity landscape. To this end, it is important to understand other countries' tactics, and most countries' cybersecurity policies focus on big picture issues such as national security, healthcare, and defense [3]. While cybersecurity technology is constantly evolving through research, cyber threat technology is also evolving. The U.S. has a number of cybersecurity research efforts to address evolving cyber threat technologies, including the National Institute of Standards and Technology's (NIST) Cybersecurity Framework,

The associate editor coordinating the review of this manuscript and approving it for publication was Alba Amato.

FIRST's The Common Vulnerability Scoring System (CVSS) 4.0, MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK), and D3FEND. In addition, various studies have been conducted to block threats with similar patterns by learning known threats through machine learning, and this is a topic that will continue to be researched in the future [4], [5], [6], [7]. However, these studies are limited to responding to new cyber threat technologies because they only enhance security with threats with similar patterns within a set defense technology. To address these issues, this study investigated how to select appropriate cybersecurity technologies against cyber threats. The metrics were designed based on MITRE's ATT&CK [8], which categorizes information about the latest cyberattack techniques into a knowledge graph, and D3FEND [9], which categorizes cybersecurity technologies. The metric can quantify the latest security technologies as updated by D3FEND and ATT&CK. To validate the designed metrics, a virtual network environment with vulnerabilities was designed. Then, cyber-attack scenarios were designed and tested. As a result, we have selected a list of cybersecurity techniques that are optimized for network environments with limited resources. This means that the proposed method can be adapted to continuously evolving network and system environments, security technologies, and threats to improve the overall security level of enterprises and countries.

This research consists of five chapters. Section II describes related work, including MITRE's attack and defense technologies that serve as the background for this research, the current state of research by various organizations and researchers, and defense policies. Section II describes the structure of the methodology proposed in this study, including the design and methodology of metrics to quantitatively measure defensive behavior against cyberattacks. Section III describes the experiments using the method, and Section IV concludes with conclusions, future research directions, and comparisons with other studies.

II. RELATED WORK

A. MITRE's ATT&CK, D3FEND

ATT&CK [8], developed by MITRE Corporation, is a framework used in the field of cybersecurity. It is designed to effectively organize and share knowledge about cyberattacks and provides a cybersecurity standard terminology and taxonomy to provide information about attacker behavior patterns and attack techniques. This allows organizations to develop defensive strategies against specific threats and attack techniques and improve detection and response to security issues. ATT&CK can be broadly categorized into Techniques, Tactics, and Defenses, with "Techniques" and "Tactics" being more related to attacks, and "Defenses" being more related to defense. Tactics represent the attacker's larger strategic goals to achieve their end goal, while Techniques describe the attack techniques as the specific actions within each Tactic. Finally, Finally, "Mitigation," a subset of "Defense," describes defenses and mitigations against specific attack techniques or tactics, providing specific actions or enhancements to detect or prevent attacks. These ATT&CKs are used by security professionals and solution developers to better understand specific attacks and develop defense strategies.

D3FEND [9] is a knowledge graph of cybersecurity countermeasures researched by MITRE, and it does not score cybersecurity technologies by defining digital artefacts, but rather breaks them down by function to help users make more accurate judgements and build security architectures. The framework is constantly being updated, and while the initial release had 5 Tactics, it now has a total of 6 Tactics and 22 sub-techniques, including Models, with further subdivisions below. The D3FEND framework can look up a relevant defense technology by its Technique ID in ATT&CK, and describes the techniques of that defense technology, as well as providing information about the associated digital artefacts. Figure 1 shows the connection between these ATT&CK and D3FEND.

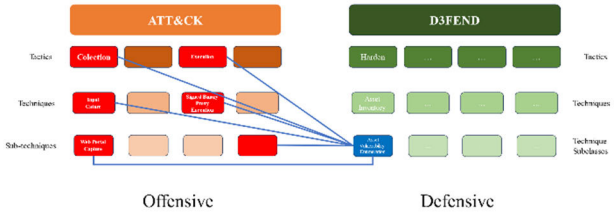


FIGURE 1. Example mapping relationship between ATT&CK and D3FEND.

B. EVALUATE CYBERSECURITY SCORES

Ahmed et al. [10] describe an empirical analysis of a cybersecurity scoring system. Security scores, which are quantitative indicators of an organization's security, generally a higher score indicates that an organization is more secure. However, these scores can vary depending on the organization providing the metric. Additionally, security scores typically use only externally accessible data and are comprised of three sources: external data, publicly available data, and proprietary algorithms. While a high security score indicates that an organization is well secured, even a high-scoring organization may be subject to more attacks than a low-scoring organization if the data it is handling is of a high level of importance compared to other organizations [11]. Therefore, while a security score can be a good indicator of security excellence and a low breach success rate, it is an assessment of an organization's overall security and may be low or too high for the level of criticality of the data [12]. As a result, to ensure fair and accurate assessments, the U.S. Chamber of Commerce has adopted six principles to guide its security ratings. These principles are shown in Figure 2. As a security rating company, BitSight uses data that feeds into a proprietary algorithm based on the six principles to generate a security score ranging from 250 to 900. The metrics consist of a compromised system score comprising five risk vectors, a diligence score focusing on management, such as security

updates to software, and a user behavior score measured by user activity.

Through this analysis, Ahmed et al. [10] point out that no two companies' networks are the same when it comes to measuring security scores, and that the number of users in a network should be considered when measuring scores. They also note that different companies face different types of threats depending on what they need to secure, so security incentives should be based on the criticality of the asset. Finally, it's important to ensure that the network infrastructure is trustworthy.

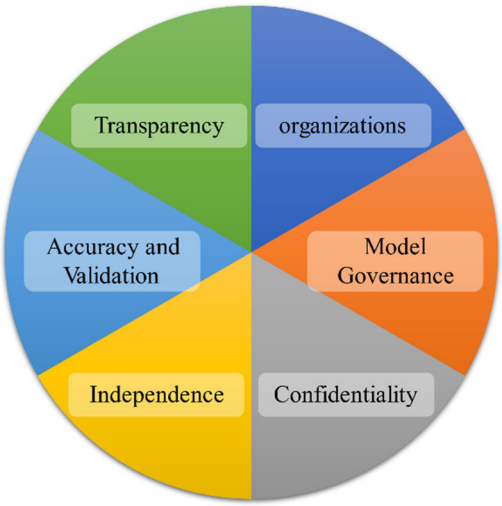


FIGURE 2. Six security rating principles adopted by the U.S. chamber of commerce.

In order to determine and benchmark the cybersecurity risk of an organization, Yampolskiy et al. [13] collected non-intrusive data related to the organization, processed the security information extracted from the collected data and calculated a security score. The calculated security score is assigned based on the correlation between the extracted security information and the overall cybersecurity risk determined by analyzing previously breached companies in the same industry. A patent has been filed to calculate an entity's overall cybersecurity risk score based on the calculated security score and as-signed weights.

C. CYBERSECURITY POLICY-RELATED PROPERTIES

Mishra et al. [14] identified 14 common cybersecurity attributes across seven countries (USA, EU, Australia, Canada, China, India, Malaysia): telecommunications, networks, cloud computing, e-commerce, online banking, smart grid, consumer rights, cybercrime, cryptography, privacy, identity theft, digital signatures, data security, and spam. While these attributes are self-contained, the interdependencies between them can be further specified for specific contexts. To combat cybercrime, the key characteristics of CS need to be identified and well-defined so that a comprehensive policy can be developed. While various stakeholders contribute to the development of CS policy, governments are the primary actors in the creation and revision of policy. Identifying common policies across countries can help academics and policymakers develop cybersecurity policies.

D. CYBERATTACK TARGETS

Cyberattacks are conducted in seven stages: reconnaissance, weaponization, dissemination, exploitation, installation, command and control, and goal achievement [15]. In addition, creating an attack graph for a target network is effective in identifying the attack path from the attack launch point to the target [16]. Identifying vulnerabilities in a network is important to prepare for cyber threats because attackers use vulnerabilities in the target network to identify the optimal attack path.

Common Platform Enumeration (CPE) is a structured naming scheme for software and packages. It consists of 11 attributes, including part, vendor, product, version, update, edition, language, and sw_edition of the software installed on the workstation, expressed as "cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x64:*". The product, version, update, target_hw, etc. of the CPE name can be used to match the corresponding vulnerability, and multiple CVEs can be matched for a single CPE [17].

Common Vulnerabilities and Exposures (CVEs) are a list of publicly known computer security flaws maintained and overseen by MITRE with financial support from the Cybersecurity and Infrastructure Security Agency (CISA). CVE IDs, the identifiers for CVEs, are assigned by the CVE Numbering Agency (CNA), which includes companies representing major IT vendors. When a security flaw is discovered, it is forwarded to the CNA, which assigns a CVE ID to the information, writes a brief description with references, and distributes it. CVE IDs are issued in the form of a CVE-Year-Serial number [18].

CVSS is an open framework that helps assess security threats by quantifying the nature and severity of software vulnerabilities. It is maintained by FIRST, an international association of incident response and security teams, and currently exists in v3.1 and v4.0 preview. CVSS has three main metrics: foundation, time, and environment, and each metric is composed of subcomponents [18]. The National Vulnerability Database (NVD) allows you to look up the CVSS score by CVE ID and provides a calculator so you can calculate it yourself. It is used by many organizations and vulnerability management programs because it can be used as an indicator of the severity of a vulnerability.

The Common Weakness Enumeration (CWE) is a list of common software and hardware vulnerability types that affect security. A vulnerability is a condition in software, firmware, hardware, and service components that can lead to vulnerability under certain circumstances. The CWE describes and discusses software and hardware weaknesses in a common language and identifies weaknesses in existing software and hardware products. It assesses the coverage of tools targeting these weaknesses and utilizes a common baseline standard for weakness identification, mitigation,

and prevention efforts [19]. These CWEs are related to MITRE's Common Attack Pattern Enumeration and Classification (CAPEC), which focuses on application security and describes common attributes and techniques used by attackers to exploit known weaknesses in cyber-enabled capabilities [20]. In addition, because CAPEC includes the technology numbering of ATT&CK, information about ATT&CK technologies can be obtained through CAPEC and vice versa.

E. CYBER SECURITY STRATEGIES

Varma [21] proposed a methodology to improve cyber resilience by integrating cyber threat detection and mitigation strategies using artificial intelligence (AI). The proposed methodology analyzes various AI-based models and algorithms to evaluate the accuracy and efficiency of cyber threat detection. It analyzes network traffic data using machine learning and deep learning techniques to detect anomalous patterns, and proposes a system that utilizes AI to detect threats in real-time and automatically execute response strategies. Measure detection rate, false positive rate, and response time as performance metrics for threat detection systems. The AI-integrated system is designed to adapt to dynamic cyber threats, and the study demonstrates that AI-based systems are effective in quickly responding to new attack vectors and enhancing an organization's security posture. The proposed system was experimentally validated using various cyber-attack scenarios, and the results showed high detection rates and low false positives compared to traditional security systems. This means that adapting to dynamic cyber threats and choosing a rapid response strategy is crucial to enhance cybersecurity.

Riggs et al. [22] categorize different types of cyber-attacks, including denial of service (DoS), ransomware, man-in-the-middle (MITM) attacks, phishing, and false data injection attacks (FDIA). The researchers also study the specific vulnerabilities associated with these attacks and the mitigation strategies to counter them. For example, DoS attacks can be mitigated through network traffic monitoring and intrusion detection systems (IDS). We proposed a defense-in-depth strategy that incorporates multiple layers of security measures to protect critical infrastructure. This approach involves using intrusion detection systems, encryption, and regular security audits to ensure the resilience of critical systems against cyber threats. They also emphasized the importance of adhering to cybersecurity standards provided by ISO and NIST, which provide frameworks and best practices for developing secure information systems. The authors noted that the rapid increase in cyberattacks on critical infrastructure requires a proactive and adaptive approach to cybersecurity, and by continually updating security measures and leveraging advanced technologies, organizations can better protect their critical assets from evolving cyberthreats.

III. METRICS DESIGN FOR DEFENSIVE SECURITY COUNTERMEASURES

This chapter suggests one metric to quantitatively assess the effectiveness of each defense measure and six metrics to calculate the score.

A. COUNTERMEASURE RECOMMENDATION METHOD PROCESS

An attack vector is created to progress an attack from the network to the cyber attacker's target asset. The assets along the attack path will have multiple vulnerabilities, and there will be multiple defenses that can be applied to the assets. It is possible to select only the vulnerabilities exploited by the attacker and select them as security measures. However, the defensive technologies included in the security countermeasures may not be the optimal security measures for each asset due to cost limitations, lack of equipment, or inability to respond quickly. It is very difficult to select cybersecurity measures while considering these various issues. Therefore, this study proposes a cybersecurity countermeasure recommendation including a three-step algorithm. The algorithm classifies only the defense technologies applicable to the network among the defense technologies identified through the vulnerabilities present in the assets, and finally recommends them through prioritization by measuring the quantitative evaluation score. As preliminary work for the algorithm, we describe the CPE-CVE-CWE-CAPEC-D3FEND mapping methodology.

1) IDENTIFYING CVES VIA CPES

Various vulnerabilities present in an asset can be identified by analyzing the network inside the organization or by knowing the program information used (vendor name, version, product name, etc.), i.e., CPE.

2) CWE MAPPING

For identified CVEs, CWEs are extracted from the 'Observed Examples' column of the CWE dataset or through the CWE-CVE root cause mapping methodology (available on the official page).

3) CWE AND ATT&CK UTILIZING CAPEC

CAPEC has CWE information in the 'Related Weakness' column and ATT&CK attack technique values as 'Entry ID' in the 'Taxonomy Mappings' column.

4) ATT&CK TO D3FEND

D3FEND officially supports mapping with ATT&CK.

By utilizing these mappings, you can effectively find defenses against CVEs identified through network analysis or CPE. The overall structure is shown in Figure 3, and the three-step algorithm is as follows.

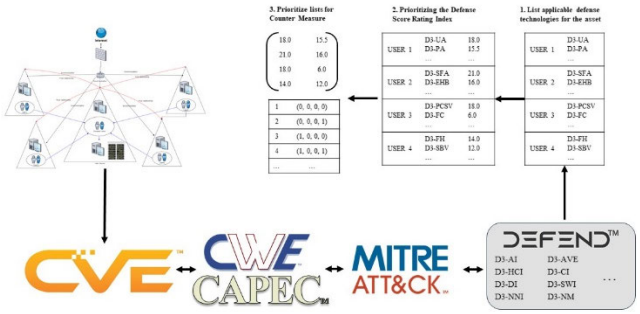


FIGURE 3. Countermeasure recommendation method process.

a: LISTING APPLICABLE DEFENSE TECHNIQUES FOR THE ASSET

Extract a list of applicable D3FEND defense techniques based on the defense techniques based on the vulnerabilities of each asset and the attacker's chosen attack technique (ATT&CK's technique) through the mapping methodology of the previous work.

b: PRIORITIZING THE DEFENSE SCORE RATING INDEX

Sort and prioritize the defense technology rating index calculated for each asset in descending order. The Defense Score Rating Index is described in III-C.

c: PRIORITIZING LISTS FOR CYBERSECURITY COUNTERMEASURES

Provide a prioritized list of defense technologies to recommend various cybersecurity countermeasures to security personnel and administrators. To achieve this, the two levels of asset-specific defense measure lists are determined into a single two-dimensional matrix, which can be prioritized by permutation [23] to provide different combinations of defense countermeasures.

The above procedure allows security personnel to select the appropriate cybersecurity measures for their network environment.

B. DESIGN AND DEFINE METRICS

Two of the six metrics are designed to be related to vulnerabilities. This is a result of accepting the importance of the security update score among the scores mentioned by Ahmed et al. [10]. The rest consisted of factors related to the network environment and position against attack techniques. The six designed metrics are as follows.

1) COST

The cost of applying defenses to your network. This includes both human and physical assets expended to apply the defense behavior. The higher the cost, the better the performance of the mitigation technique, but it is not directly proportional, so it is a good metric for selecting defenses that perform well at a lower cost. The lower the cost, the higher the score.

2) DEFENSE PHASE

Based on the four phases of breach incident response (IR) proposed by the US NIST [24] and the incident response phase consisting of a six-step process proposed by Kral in [25], it is composed of four phases: detection, initial response, recovery response, and investigation and analysis.

3) LEVEL OF DIFFICULTY

The concept of the difficulty of applying defense techniques, which is calculated based on the vulnerability of the asset in the network environment. Vulnerability is calculated based on CVSS and can be measured based on CVSS prediction algorithms [26] for new CVEs due to the constantly evolving cyberspace.

4) ASSET POSITION IN ATTACK PATH

This score is measured by determining the location of network assets targeted by detected threats along the attack path, from the attack launch point to the end goal. If you can proactively stop the threat at an asset close to the origin of the attack, you will score high.

5) EFFECT SCORE

A measure of the effectiveness of a defense technology when applied to a network environment. It is measured by the likelihood that a vulnerability in the network will be eliminated by applying the defense. The effectiveness metric, like the difficulty metric, is based on the CVSS prediction algorithm, which can respond to new vulnerabilities.

6) APPLICABILITY TIME

Ensuring that you can quickly apply defenses and stop threats from the point of attack detection is critical to improving cybersecurity, hence the metric that measures the time it takes to apply defense technique.

7) SINGLE DEFENSE SCORE

The above six metrics are equally weighted, and the higher the score of the remaining metrics relative to the cost metric, the higher the defense evaluation index.

C. CALCULATION METHOD

The six metrics are calculated as follows, and after all calculations, they must be normalized to the same range of values to produce the Defense Assessment Index.

1) COST

It is measured by the network assets, human assets of the network to which the defense technology is applied and is measured by the judgement of the managers and experts of the organization, or by the amount of hiring security experts. However, if the defensive technology is related to security equipment, the cost is calculated by including the cost of such equipment if the organization does not own such equipment, and the human cost is calculated.

When measuring costs, you should consider the following First, the amount of money available depends on the purpose of use (defense, private enterprise, etc.), network environment, security equipment you have, etc. The second is. it is not fixed due to many variables: labor costs, fluctuating market prices of resources, etc. For this reason, it can be measured differently depending on when it is measured and who is measuring it.

The calculated cost is normalized using the min-max normalization algorithm by finding the maximum and minimum cost of all defense technologies. (0 <= Cost <= 1).

2) DEFENSE PHASE

As mentioned in Section III-B, there are four phases and identify the defense phases that can be applied to each defense technique. A defense technique can have multiple defense phases, but for the purposes of this study, it is assumed to have a maximum of two defense phases. Each defense phase is scored from 1 to 5, with detection (4), initial response (5), recovery response (3), and investigation and analysis (1). (1 <= Phase <= 5).

Detection is a defense focused on identifying and alerting to cyber threats and can include network traffic analysis, log monitoring, and anomaly detection. Initial Response is the immediate action taken immediately after a threat is detected. This could be adjusting firewall rules, tightening access controls, or quarantining malicious code. Recovery Response involves steps to repair the damage, such as restoring data backups, reconfiguring systems, and patching vulnerabilities. Investigation and Analysis: Steps to determine the cause of the attack and prevent the same type of attack in the future. Examples include forensic analysis, log analysis, and threat intelligence research.

3) LEVEL OF DIFFICULTY (LVL)

The more vulnerabilities an asset has, the more difficult it is to apply defensive techniques. It is calculated as the sum of the vulnerability scores corresponding to the asset ($AssetCVSS_n$) over the sum of the scores of all vulnerabilities in the attack path ($\sum AssetCVSS$) as shown in Eq. 1. (0 <= Lvl <= 10)

$$Lvl = AssetCVSS_n / \sum AssetCVSS \tag{1}$$

4) ASSET POSITION IN ATTACK PATH (POSITION)

It is measured based on the position of the asset on the cyber attacker's attack path and is calculated as the position of the selected asset relative to the total number of assets on the path. (0 <= Position <= 1).

5) EFFECT SCORE

Based on the vulnerabilities of the asset, it is calculated as the CVSS average of the vulnerabilities after eliminating the vulnerabilities corresponding to the defense technology among the vulnerabilities existing in the asset through the relationship of CPE-CVE-CWE-CAPEC-ATT&CK-D3FEND as shown in Eq 2. (0 <= Effect <= 10).

6) APPLICABLE TIME (TIME)

Calculates the effectiveness of a mitigation technique over the time it takes to apply and complete. If the defensive action can be applied immediately, the effect is good, and the closer the calculated value is to 1, the greater the effect. It is calculated from the time of application, completion, and detection of the at-tack, and the variables as shown in Table 1 are defined based on Minute and calculated as shown in Eq 2. (0 <= Time <= 1)

$$Time = 1 - (TimeDA - TimeAD)/(TimeDC - TimeAD) \tag{2}$$

TABLE 1. The time matric calculations method's parameter and definitions.

Parameter	Definition
$Time_{DA}$	When to apply mitigation techniques
$Time_{DC}$	When defense techniques are applied
$Time_{AD}$	When the attack was detected

7) NORMALIZATION

The above metrics cannot be calculated with the same weight be-cause they all have different ranges of values, so they are normalized to make all the metrics equal, with values between 1-5.

Figure 4 shows how to replace values between 0-1 with values in the range 1-5. Values between 0 and 10 are replaced with values in the range 1-5 by multiplying the value below (the raw value before normalization) by 10.

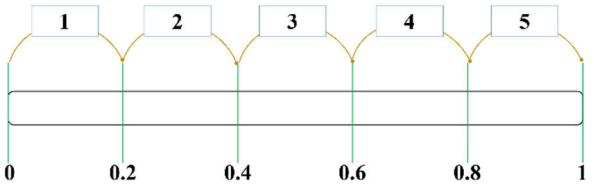


FIGURE 4. Normalization methods.

8) SINGLE DEFENSE SCORE (DS)

The higher the sum of the other metrics relative to the cost, the higher the score. The calculation method is shown in Eq 3.

$$DS = (Step + Lvl + Position + Effect + Time)/Cost \tag{3}$$

The above formula for calculating the defense evaluation index can be further refined by adding weights to the indicators based on the judgement of managers and experts.

Figure 5 is an example of network information and attack scenarios for selecting cybersecurity measures. Figure 6 is an example of a prototype showing the cybersecurity countermeasure priorities calculated based on Figure 5 and the defense techniques included in the countermeasure.

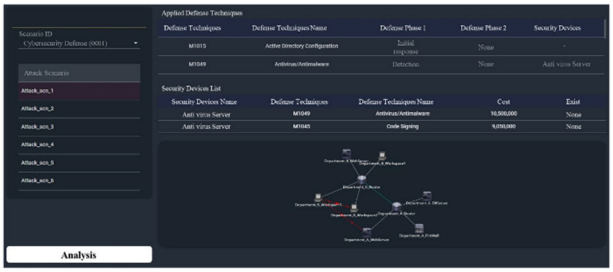


FIGURE 5. Examples of network information and attack vectors.

FIGURE 6. Cybersecurity countermeasures list and examples of defensive technologies included in the cybersecurity countermeasures.

IV. EXPERIMENTS

Due to the unreliability of the prototype, we conducted a logical experiment to verify the proposed method. For this purpose, we constructed a network for experiments. After performing scenarios with cyber-attack vectors on the configured network, we applied the proposed method to verify the results.

A. DESIGNING A NETWORK CONFIGURATION

Design a network for the experiment. The target networks of this study are military networks and corporate networks. Because using a real network environment may leak the organization's vulnerabilities and network information, we constructed a virtual network in this paper. However, in real-world implementations, vulnerability information and attack paths should be measured by security personnel, while other metrics can be helped by external organizations.

Fencl et al. [27] describe an algorithm for network topology design, noting that randomizing the network design can lead to problems with data transmission time delays and topology configuration costs. In addition, the design of network topology is important because if the network is poorly designed, it cannot be guaranteed to be safe from various cyber threats. In addition, conducting experiments to conduct various analyses in a virtual network environment similar to the real network environment is an important step to evaluate the advantages and ultimately deploy the solution before actually using it [28]. Therefore, in this study, we built a virtual network environment rather than a real network environment to conduct our experiments. Although the virtual network environment we designed is based on a private network, the methodology in this study can be applied to different types of networks, including closed networks with limited access and enhanced security measures, corporate networks, and public networks. This adaptability means that the proposed defense metrics can effectively protect against cyber threats regardless of the architecture or accessibility of the network. Conducting experiments in virtual network environments not only mitigates the potential risks associated with real-world testing, but also demonstrates the versatility of the approach to accommodate the unique requirements and challenges presented by different network environments.

The main experiments were conducted in a military network-based virtual environment, a small organization network; however, the military network-based environment is not disclosed in this paper. Therefore, we use a small office/home office network environment designed based on [29], [30], and [31]. Table 2 summarizes the elements required in the designed network, and the designed network is shown in Figure 7.

TABLE 2. Using network topology components.

Component	Example	Required scope
Network devices	Workstation, Printer, Laptop, Switch, etc.	Workstation, Printer, Switch, Server, Router, DB Server
Security devices	Fire Wall, IDC, IPS, etc.	All
Communication information	Packet, Delay time, Connection information, etc.	Connection information
System information	IP, Software information, Data file, User information, etc.	CVE

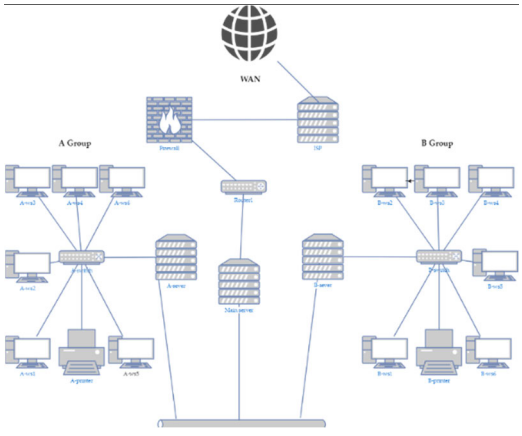


FIGURE 7. Designed network topology.

B. DESIGN ATTACK SCENARIOS

In order to compare the before and after of the proposed method, a cyber-attack must occur. By creating and performing a cyber-attack scenario, it is possible to identify the vulnerability of the network, and by performing the cyber-attack scenario again after applying the proposed

method, it is possible to identify the enhancement of cybersecurity. In addition, in order to demonstrate that the proposed method is a universal method and can be used in various environments, the attack scenarios are subject to the following assumptions and restrictions.

1) Based on ATT&CK's attack techniques, an attacker can use any attack technique that corresponds to the vulnerabilities present in the network. Utilize available attack techniques based on the CVE to D3FEND mapping method mentioned in III-A.
2) Cyber-attack attempts have a 100% success rate and can only be defended by D3FEND's defense technology. This is to evaluate the pure effectiveness of the defense technology by ensuring that it is not affected by rulesets such as security equipment or physical security.
3) To reach the final target network asset, the attack must traverse at least three assets, which means the minimum attack path is three hops, and is designed to allow the attack to progress through a variety of paths.
4) Based on the network topology designed in Section IV-A, the attacker goes through B-ws2, B-ws3, and A-ws5 to reach the final attack target (A-ws4). Figure 8 shows the CPE of the designed network Workstation and some of the CVEs corresponding to the CPE. Furthermore, the defense techniques applied are shown in Table 3 and the attack path is shown in Figure 9. The yellow line shows the direct access path from the network, and the red arrow line shows the flow of the attack path.

List of CPEs on a workstation

workstation name	CPE	vendor	product	version	target HW
A-ws1	cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x64:*	Microsoft	Outlook	2013	x64
A-ws1	cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x64:*	Microsoft	Office	2013	x64
A-ws2	cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x64:*	Microsoft	Outlook	2013	x64
A-ws2	cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x64:*	Microsoft	Office	2013	x64
A-ws3	cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x64:*	Microsoft	Outlook	2013	x64
A-ws3	cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x86:*	Microsoft	Office	2013	x86
A-ws4	cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x86:*	Microsoft	Outlook	2013	x86

List of CVEs mapped to CPEs

CPE	CVE
cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x64:*	CVE-2023-35311, CVE-2017-17689, CVE-2018-0850, CVE-2013-3905, CVE-2007-4040, CVE-2006-6659, CVE-2000-0216, CVE-2000-0160
cpe:2.3:a:microsoft:outlook:2013:-:-:*:-:-:x86:*	CVE-2023-35311, CVE-2017-17689, CVE-2018-0850, CVE-2013-3905, CVE-2007-4040, CVE-2006-6659, CVE-2000-0216, CVE-2000-0160
cpe:2.3:a:microsoft:outlook:2016:*:*:*:*:*:x64:*	CVE-2023-36763, CVE-2023-36893, CVE-2022-35742, CVE-2021-31949, CVE-2021-28452, CVE-2020-17119, CVE-2019-1084, CVE-2019-1200
cpe:2.3:a:microsoft:outlook:2016:*:*:*:*:*:x86:*	CVE-2023-36763, CVE-2023-35311, CVE-2023-33131, CVE-2021-31949, CVE-2020-16949, CVE-2020-16947, CVE-2020-1483, CVE-2019-1200, CVE-2019-1084
cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x64:*	CVE-2014-1808, CVE-2014-1756, CVE-2014-2730, CVE-2013-5054, CVE-2013-1324, CVE-2013-3889, CVE-2007-3282, CVE-2007-3109, CVE-2006-4694, CVE-2004-0848
cpe:2.3:a:microsoft:office:2013:-:-:*:-:-:x86:*	CVE-2014-6362, CVE-2014-6364, CVE-2014-1809, CVE-2014-1756, CVE-2013-1324, CVE-2013-3889, CVE-2007-3282, CVE-2006-1311, CVE-2005-2127
cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:x64:*	CVE-2023-36413, CVE-2023-41764, CVE-2023-36896, CVE-2022-38048, CVE-2022-34717, CVE-2022-22003, CVE-2022-21841

FIGURE 8. The CPE of a designed network workstation (left) and some of the CVEs corresponding to the CPE (right).

These assumptions and limitations allow us to evaluate different cyber-attack scenarios and demonstrate the validity of the proposed methodology. By using different attack types, we can quantitatively evaluate and compare the effectiveness of defense techniques in a network environment.

C. APPLYING THE METHOD

Three of the six indicators in the proposed methodology include the presence of defense equipment and the amount of money spent on defense technologies. Therefore, in order to calculate a single defense score, a preparatory step is required to pre-calculate the three indicators. The preparation phase has the following prerequisites and assumptions.

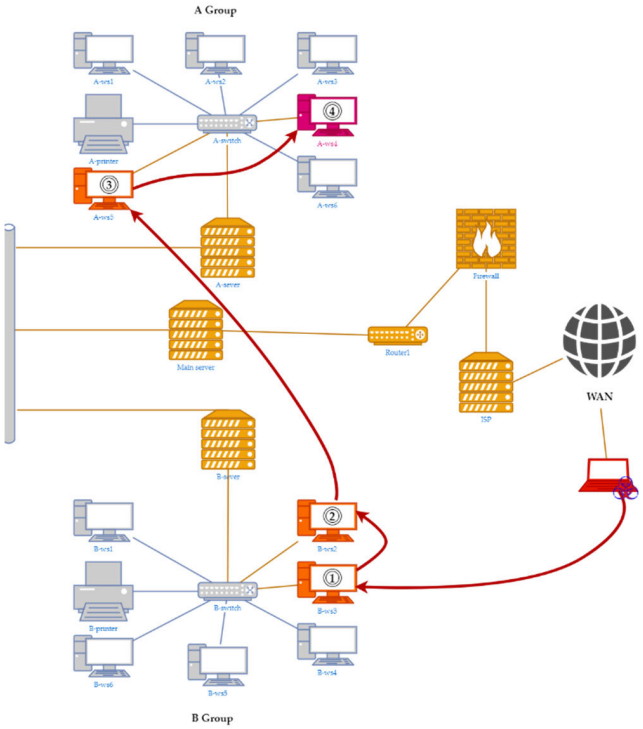


FIGURE 9. Designed attack scenario and route.

TABLE 3. List of defense techniques applied across the network.

Defense Techniques	Description	Device
D3-DNSDL	DNS Access Exclusion Policy	Firewall
D3-NTF	Network traffic filtering	Firewall
D3-BA	Authentication before bootloader programs	Workstations
D3-DE	Disk encryption	Workstations

1) COST

This is fluid as it includes the amount of human resources and equipment, so for the sake of fairness, all costs are calculated at the same amount. However, if defensive equipment is required, the cost of purchasing defensive equipment is taken into account. However, as mentioned in Section III-C, this would result in 0 and 1 for MIN-MAX normalization and 0 and 5 for the defense evaluation index, so we assumed a score of 5 for defense technologies that do not require security equipment and a score of 3 for defense technologies that require security equipment.

2) DEFENSE PHASE

You must set a Defense Phase for each Defense Technique. Set a minimum of one and a maximum of two defense skills.

TABLE 4. Summary of study comparisons.

Proposed Method	Important METRIC	Scope of use	Attack Type Coverage
J. Ahmed et al. [10]	Asset Criticality, Network Reliability, Number of network users	Organization	Botnet Infection, Spam, Malware Server, Unsolicited Communication
Stacy Collett [11]	Data Criticality	Organization	Not specified
Yampolskiy et al. [13]	About Data Security, Weight	Organization	Social Engineering Attacks, Malware, Botnet ifections, Hacker Sites
A. Mishra et al. [14]	Key Common Characteristics of Cybersecurity	Government	DoS, Cybercrime during COVID-19, Cross-border Cyber threats, Attacks on critical infrastructure
V. V. Varma. [21]	Connectivity, Communication Protocols	Organization	DDoS, IP Spoofing
H. Riggs, et al. [22]	Vulnerability Analysis, Anomaly Detection	Organization, Government	Ransomware, APTs
Proposed Method	Future-proofing Technologies, Flexible, Network Environment	Private, Organization, Government	DDoS, IP Spoofing, Brute Force

This is determined based on the description of the defense technology.

D3FEND ID	D3FEND Tactic	D3FEND Technique	D3FEND Technique Level 0 Name	Description
D3-DENCR	Harden	Platform Hardening	Disk Encryption	Disk Encryption
D3-BA	Harden	Platform Hardening	Bootloader Authentication	Authentication Before Bootloader Programs
D3-ANAA	Detect	Network Traffic Analysis	Administrative Network Activity Analysis	Analyze administrator network activity
D3-CA	Detect	Network Traffic Analysis	Certificate Analysis	Analyze network certificate health
D3-CSPP	Detect	Network Traffic Analysis	Client-server Payload Profiling	Analyze request and response packets to identify normal ranges and derive anomalies
D3-DNSTA	Detect	Network Traffic Analysis	DNS Traffic Analysis	Analyze DNS traffic to identify malicious behavior
D3-FC	Detect	Network Traffic Analysis	File Carving	Extract files from network traffic
D3-IPCTA	Detect	Network Traffic Analysis	IPC Traffic Analysis	Analyze IPC traffic (Ex: SMB)
D3-NTCD	Detect	Network Traffic Analysis	Network Traffic Community Deviation	Check frequently communicated sites and then check when accessing anomalous sites
D3-PHDURA	Detect	Network Traffic Analysis	Per Host Download-Upload Ratio Analysis	Analyze download/upload bandwidth range by host
D3-PMAD	Detect	Network Traffic Analysis	Protocol Metadata Anomaly Detection	Check network protocols for abnormalities (Ex: headers, request/response times)
D3-RTSD	Detect	Network Traffic Analysis	Remote Terminal Session Detection	Analyze remote terminal session access
D3-RTA	Detect	Network Traffic Analysis	RPC Traffic Analysis	Analyze remote procedure calls
D3-CAA	Detect	Network Traffic Analysis	Connection Attempt Analysis	Analyze the number of connection attempts
D3-ISVA	Detect	Network Traffic Analysis	Inbound Session Volume Analysis	Analyze access request session volume
D3-BSE	Detect	Network Traffic Analysis	Byte Sequence Emulation	Analyze shell code in network packets
D3-RPA	Detect	Network Traffic Analysis	Relay Pattern Analysis	Check for anomalies in external connections using proxies, forwarding, routing, etc.
D3-UDTA	Detect	User Behavior Analysis	User Data Transfer Analysis	Analyze user transferred data volumes
D3-DNSAL	Isolate	Network Isolation	DNS Allowlisting	DNS allow policy
D3-DNSDL	Isolate	Network Isolation	DNS Denylisting	DNS access exclusion policies
D3-EAL	Isolate	Execution Isolation	Executable Allowlisting	Executable allowlist
D3-PT	Evict	Process Eviction	Process Termination	Process termination

D3FEND ID	Cost	Defense Phase1	Defense Phase2	Applicable time	Applied Seq	Complate Seq
D3-DENCR	$100,000	2(Initial response)	-	0.65	$TIME_{AD}+4$	$TIME_{DA}+3$
D3-BA	$100,000	2(Initial response)	1(Detection)	0.75	$TIME_{AD}+3$	$TIME_{DA}+2$
D3-ANAA	$100,000	3(Investigative Analysis)	-	0.6	$TIME_{AD}+4$	$TIME_{DA}+4$
D3-CA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-CSPP	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+2$	$TIME_{DA}+5$
D3-DNSTA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+2$	$TIME_{DA}+5$
D3-FC	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-IPCTA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+2$	$TIME_{DA}+5$
D3-NTCD	$100,000	3(Investigative Analysis)	-	0.8	$TIME_{AD}+2$	$TIME_{DA}+2$
D3-PHDURA	$100,000	3(Investigative Analysis)	-	0.7	$TIME_{AD}+3$	$TIME_{DA}+3$
D3-PMAD	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-RTSD	$100,000	3(Investigative Analysis)	-	0.6	$TIME_{AD}+4$	$TIME_{DA}+4$
D3-RTA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-CAA	$100,000	3(Investigative Analysis)	-	0.7	$TIME_{AD}+3$	$TIME_{DA}+3$
D3-ISVA	$100,000	3(Investigative Analysis)	-	0.75	$TIME_{AD}+2$	$TIME_{DA}+3$
D3-BSE	$100,000	3(Investigative Analysis)	-	0.55	$TIME_{AD}+5$	$TIME_{DA}+4$
D3-RPA	$100,000	3(Investigative Analysis)	-	0.65	$TIME_{AD}+3$	$TIME_{DA}+4$
D3-UDTA	$100,000	3(Investigative Analysis)	-	0.7	$TIME_{AD}+2$	$TIME_{DA}+4$
D3-DNSAL	$110,000	1(Detection)	4(Recovery)	0.85	$TIME_{AD}+2$	$TIME_{DA}+1$
D3-DNSDL	$110,000	1(Detection)	4(Recovery)	0.85	$TIME_{AD}+2$	$TIME_{DA}+1$
D3-EAL	$110,000	2(Initial response)	4(Recovery)	0.85	$TIME_{AD}+1$	$TIME_{DA}+2$
D3-PT	$110,000	4(Recovery)	-	0.95	$TIME_{AD}+0$	$TIME_{DA}+1$

FIGURE 10. Three metrics set in the preparation phase: cost, defense level, and time to apply.

3) APPLICABLE TIME

The time from the time of application of the defense technology to the completion of application depends on the ability of the security expert applying the defense technology and the possession of defense equipment. Therefore, this study assumes that all defense equipment is possessed and is calculated based on the Description. It is also assumed that the time from the time of attack detection to the application of the defense technology and the time from the start of application of the defense technology to the completion of application are performed by one security expert.

The Figure 10 shows some of the metric values for the Preparation phase based on the above prerequisites and assumptions.

After all the preparations, we identified the optimal security countermeasures for the attack vectors shown in Figure 9, and the prioritized defense countermeasures for each asset are shown in Figure 11. In B-ws3, A-ws5, and A-ws4, D3-FE, a defense technology related to file encryption, scored the highest, and D3-EDL, which blocks file execution through poli-cy changes, scored the second highest.

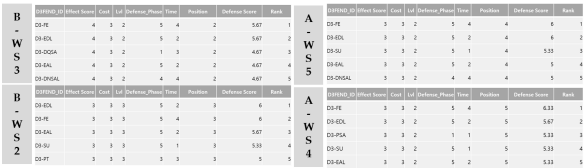


FIGURE 11. Table of defense technology prioritization results for assets.

Based on the workstation's list of defense technologies, the best security countermeasure produced by the permutation was the addition of D3-FE alone (Total 24.0), while the combination of permutations that removed duplicates from all four workstations yielded a score of 22.67: D3-FE (5.67), D3-EAL (5.67), D3-EDL (6.00), and D3-SU (5.33).

V. CONCLUSION

The purpose of this research is to provide effective and efficient security countermeasures for multiple assets with less effort in preparation for cyberattacks or in the event of damage caused by cyber-attacks. Furthermore, this research aims to prepare for the evolving cyber threats in the evolving cyberspace. To validate this, a virtual network environment was built, attack scenarios were written, and experiments were conducted. When cybersecurity countermeasures were selected through the process shown in Figure 4, it was found

that in the case of a small network with fewer paths, only one additional security technology was selected, but it was found to be the most efficient security technology in that network environment. By reversing the mapping relationship of ATT&CK-CAPEC-CWE-CVE-CPE with the defense technologies identified in the experimental results, we found that on average, more than 10 vulnerabilities can be compensated out of the average number of 16.75 vulnerabilities in the assets. We further experimented in a real-world network environment using 10 workspaces and found that they were able to cover an average of 5.4 out of 10 vulnerabilities, which was not significantly different from the results in the virtual environment.

Based on the experimental results, we compared the differences with previous studies. Ahmed et al. [10] emphasized the importance of measuring security scores based on the criticality of assets and network trust. While scores measured by security scoring companies are important, it is important to evaluate the criticality of the data because the criticality of the data determines the likelihood of being targeted by an attacker. Yampolskiy et al. [13] measured the security risk score by collecting data and extracting security information to determine the cybersecurity risk of a company, and Mishra et al. [14] stated that it is important to identify the main characteristics of common CS to develop cyber policies. Varma [21] emphasized the use of AI in cybersecurity to integrate threat detection and mitigation strategies. He designed an AI-integrated system to adapt to dynamic cyber threats and focuses on learning to quickly respond to new attack vectors and strengthen the organization's security posture. Riggs et al. [22] mention the need to incorporate multiple layers of security measures against various cyber threats. In conclusion, most cybersecurity strategy and response techniques studies emphasize collecting network security information, data information, etc. to measure cybersecurity scores in order to prepare for cyber threats. They also emphasize the use of AI techniques to perform automated response strategies to improve cybersecurity.These studies may not be universal and may not be prepared for new threats, and it may be difficult for administrators to justify the response strategies implemented by leveraging AI to perform response strategies or to modify response strategies based on the situation. However, in this study, we used ATT&CK, D3FEND, a knowledge graph-based framework of offensive and defensive techniques that is universal, continuously updated, and adaptable to new threats. We also designed, quantified, and prioritized six metrics for defensive techniques to allow for flexibility in modifying and selecting defensive strategies. This is one of the ways to select the right security measure for the network according to the evolving cybersecurity and attack technologies. In addition, we included CVEs and CVSS in the metrics, which are used globally to measure the security risk of network assets, so it can be used in various environments (individuals, organizations, countries, etc.). Table 4 summarizes a comparison of the results of these studies.

This research aims to help individuals, organizations, countries, etc. select efficient security measures with less effort in the modern world where cybersecurity is becoming increasingly important. To select efficient security measures, we proposed six metrics that can be set by users and automatically calculated according to different environments. We also indexed each column and generated permutations to prioritize them, and applied different defense techniques by removing redundancies, which means that the proposed cybersecurity mitigation procedures can be effectively applied in different network environments. The practical application of the method proposed in this study requires sufficient knowledge of the network environment, and providing this information to an external party may cause greater threats. Therefore, we mainly conducted experiments in a virtual network environment, and confirmed that it can be applied in an environment similar to a real network. For practical application, the administrator should be in charge, and the remaining indicators except vulnerability information and location information along the attack path can be helped by external personnel. In addition, efficiently utilizing frameworks that are continuously updated by leveraging CVSS prediction algorithms [26] or through APIs provided by frameworks (D3FEND, ATT&CK, CVE, etc.) can help adapt to evolving cyber threats. Therefore, the methodology proposed in this study has the following advantages. 1. by using a continuously updated framework and using a commonly used vulnerability management system, it is easy to manage the latest attack, defense, and vulnerability data. 2. By designing and quantitatively evaluating six metrics for defensive technologies, it is possible to understand why defensive technologies are recommended. Personnel can utilize them and use them as a basis for decision making. 3. The proposed methodology can be automated and used after the first network information collection. Finally, it is flexible, as the metrics are measured differently depending on the network information analyzed, and can be used in different network environments. However, this study has some limitations. First, all the frameworks used as mapping relationships may not be well matched due to their continuous updates. Furthermore, they will be unusable if they stop updating. Second, we need to collect system and network information about all the assets that make up the network in order to measure the designed metrics. Finally, while we tried to objectify the network used in our experiments, we conducted our experiments primarily in a virtual environment, which may lead to errors in generalization. In order to weight the designed metrics, it is essential to create various cyber-attack scenarios, collect data through extensive experiments, and then utilize machine learning models to identify and weight metrics that have a real impact on enhancing cybersecurity.

REFERENCES

[1] A. F. Brantly, "The cyber deterrence problem," in *Proc. 10th Int. Conf. Cyber Conflict (CyCon)*, Tallinn, Estonia, May 2018, pp. 31–54.

[2] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity enterprises policies: A comparative study," *Sensors*, vol. 22, no. 2, p. 538, Jan. 2022.

[3] T. Rajaretnam, "A review of data governance regulation, practices and cyber security strategies for businesses: An Australian perspective," *Int. J. Technol. Manage. Inf. Syst.*, vol. 2, no. 1, pp. 1–17, 2020.

[4] A. R. Ugale and A. D. Potgantwar, "Anomaly based intrusion detection through efficient machine learning model," *Int. J. Electr. Electron. Res.*, vol. 11, no. 2, pp. 616–622, Jun. 2023, doi: 10.37391/ijeer.110251.

[5] M. S. Akhtar and T. Feng, "Malware analysis and detection using machine learning algorithms," *Symmetry*, vol. 14, no. 11, p. 2304, Nov. 2022, doi: 10.3390/sym14112304.

[6] H. Jiwon, H. Kim, S. Oh, Y. Im, H. Jeong, and H. Kim, "Client-based web attacks detection using artificial intelligence," 2023. Accessed: Jul. 26, 2024, doi: 10.21203/rs.3.rs-2920883/v1. [Online]. Available: https://assets-eu.researchsquare.com/files/rs-2920883/v1_covered_9fd4d387-50c6-49d2-bde6-88f9b563c434.pdf?c=1711504235

[7] T. Z. Difaizi, O. P. L. Camille, T. C. Benhura, and G. Gupta, "URL based malicious activity detection using machine learning," in *Proc. Int. Conf. Disruptive Technol. (ICDT)*, Greater Noida, India, May 2023, pp. 414–418.

[8] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," MITRE Corp., Richmond, VA, USA, Tech. Rep. MP180360R1, 2018. Accessed: Jan. 4, 2024. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf

[9] P. E. Kaloroumakis and M. J. Smith, "Toward a knowledge graph of cybersecurity countermeasures," M.S. thesis, MITRE Corp., 2021. Accessed: Jan. 4, 2024. [Online]. Available: https://d3fend.mitre.org/resources/D3FEND.pdf

[10] J. Ahmed. (2019). *Empirical Analysis of a Cybersecurity Scoring System*. Accessed: Jan. 4, 2024. [Online]. Available: https://digitalcommons.usf.edu/etd/7722

[11] S. Collett. (2016). *Whats in a Security Score?*. Accessed: Jan. 4, 2024. [Online]. Available: https://www.csoonline.com/article/557289/what-s-in-a-security-score.html

[12] J. Vijayan. (2014). *Target Attack Shows Danger of Remotely Accessible HVAC Systems*. Computerworld. Accessed: Jan. 4, 2024. [Online]. Available: https://www.computerworld.com/article/2487452/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html

[13] A. Yampolskiy, R. Blackin, A. Heid, and S. Kassoumeh, "Calculating and benchmarking an entity's cybersecurity risk score," U.S. Patent 10 498 756, Nov. 22, 2016. [Online]. Available: https://patents.google.com/patent/US20160173521A1/en

[14] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Comput. Secur.*, vol. 120, Sep. 2022, Art. no. 102820, doi: 10.1016/j.cose.2022.102820.

[15] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in *Leading Issues in Information Warfare & Security Research*, vol. 1, Washington, DC, USA: API, 2011, pp. 113–125.

[16] I. Kotenko and A. Chechulin, "A cyber attack modeling and impact assessment framework," in *Proc. 5th Int. Conf. Cyber Conflict (CYCON)*, Tallinn, Estonia, Jun. 2013, pp. 1–24.

[17] B. A. Cheikes, D. Waltermire, and K. Scarfone, "Common platform enumeration: Naming specification version 2.3," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 7695, 2011, doi: 10.6028/NIST.IR.7695. [Online]. Available: https://www.nist.gov/publications/common-platform-enumeration-naming-specification-version-23

[18] M. Adam et al. (2019). *Common Vulnerability Scoring System (CVSS) Version 3.1: Specification Document*. Accessed: Jan. 4, 2024. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

[19] S. Christey and C. Harris. (Oct. 2009). *Introduction to Vulnerability Theory*. MITRE. [Online]. Available: https://cwe.mitre.org/documents/vulnerability_theory/CWE-Introduction_to_Vulnerability_Theory.pdf

[20] N. Amon and J. Baker. (2021). *Security Control Mappings: A Starting Point for Threat-Informed Defense*. MITRE-Engenuity. Accessed: Jan. 4, 2024. [Online]. Available: https://medium.com/mitre-engenuity/security-control-mappings-a-starting-point-for-threat-informed-defense-a3aab55b1625

[21] V. V. Varma, "Enhancing cyber resilience by integrating AI-driven threat detection and mitigation strategies," *Trans. Latest Trends Artif. Intell.*, vol. 4, no. 4, 2023. Accessed: Jul. 7, 2024. [Online]. Available: https://ijsdcs.com/index.php/TLAI/article/view/396

[22] H. Riggs, S. Tufail, I. Parvez, M. Tariq, M. A. Khan, A. Amir, K. V. Vuda, and A. I. Sarwat, "Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure," *Sensors*, vol. 23, no. 8, p. 4060, Apr. 2023. Accessed: 2024-06-07. [Online]. Available: https://www.mdpi.com/1424-8220/23/8/4060

[23] R. Arboretti, S. Bonnini, L. Corain, and L. Salmaso, "A permutation approach for ranking of multivariate populations," *J. Multivariate Anal.*, vol. 132, pp. 39–57, Nov. 2014, doi: 10.1016/j.jmva.2014.07.009.

[24] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," NIST, Special Publication 800.61, Tech. Rep. SP 800-61 Rev. 2, 2012, doi: 10.6028/NIST.SP.800-61r2.

[25] P. Kral. (2011). *The Incident Handlers Handbook*. Sans Institute. Accessed: Jan. 4, 2014. [Online]. Available: https://sansorg.egnyte.com/dl/6Btqoa63at

[26] M. R. Shahid and H. Debar, "CVSS-BERT: Explainable natural language processing to determine the severity of a computer security vulnerability from its description," in *Proc. 20th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Pasadena, CA, USA, Dec. 2021, pp. 1600–1607, doi: 10.1109/ICMLA52953.2021.00256.

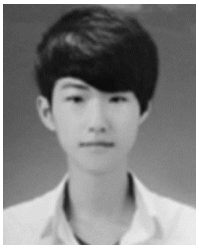
[27] Fencl et al., "Network topology design," *Control Eng. Pract.*, vol. 19, no. 11, pp. 1287–1296, 2011.

[28] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford, "In VINI veritas: Realistic and controlled network experimentation," in *Proc. Conf. Appl., Technol., Architectures, Protocols Comput. Commun.*, Italy, Aug. 2006, pp. 3–14, doi: 10.1145/1159913.1159916.

[29] L. Yang and Y. Ding, "The design of network topology big data platform in cloud computing," in *Proc. 2nd Int. Conf. Adv. Technol. Intell. Control, Environ., Comput. Commun. Eng. (ICATIECE)*, Bangalore, India, Dec. 2022, pp. 1–5, doi: 10.1109/ICATIECE56365.2022.10047353.

[30] J. L. Harrington, "Part two: Design and connectivity," in *Ethernet Networking for the Small Office and Professional Home Office*. Amsterdam, The Netherlands: Elsevier, 2010.

[31] W. Odom, *CCNA 200-301 Official Cert Guide*, vol. 2. Indianapolis, IN, USA: Cisco Press, 2019, Accessed: Jan. 4, 2024. [Online]. Available: https://www.cefracor.org/sites/www.cefracor.org/files/webform/documents/offre-complete/fichier/pdf-ccna-200-301-official-cert-guide-library-wendell-odom-pdf-download-free-book-eee99cc.pdf



JANG JISOO received the B.S. degree in computer science from Seoul Hoseo Occupational Training College, Seoul, South Korea, in 2021, and the M.S. degree in computer science from Sejong University, Seoul, in 2023, where he is currently pursuing the Ph.D. degree. From 2017 to 2019, he was an alternative to military service with a real estate company in South Korea, where he was responsible for website development and maintenance. His research interests include machine learning, cyberspace, cyber warfare, and military science.

SUBONG JUNG received the B.S. degree in electronic engineering from the Naval Academy, Gyeongsangnam-do, Republic of Korea, in 1993, and the M.S. degree in industrial engineering from Kyung Hee University, Suwon, Republic of Korea, in 2001. He is currently a Manager with the Defense Future Technology Research Institute, LIG Systems, Seoul, Republic of Korea. His research interests include cyber warfare, decision-making, and information protection.

MYUNGKIL AHN received the B.S. degree in information and communication engineering from Chungnam National University, Daejeon, Republic of Korea, in 1997, the M.S. degree in computer engineering from Sogang University, Seoul, Republic of Korea, in 2003, and the Ph.D. degree in electrical and electronics engineering from Chung-Ang University, Seoul, in 2021. She is currently a Principal Researcher with the Cyber Technology Center, Agency for Defense Development, Seoul. Her research interests include computer security and cyberwarfare modeling and simulation.

DONGHWA KIM received the B.S. and M.S. degrees from the School of Electrical Engineering, Korea University, Seoul, Republic of Korea, in 2004 and 2007, respectively. He is currently pursuing the Ph.D. degree in computer engineering with Sejong University. He is a Senior Researcher with the Cyber Technology Center, Agency for Defense Development, Seoul. His research interests include cybersecurity training systems, M&S systems, and cyber red/blue team automation.

JAEPIL YOUN received the B.S. degree in computational information processing from the Korea Army Academy at Yeongcheon (KAAY), Republic of Korea, in 2008, the M.S. degree in cybersecurity from Ajou University, Suwon, Republic of Korea, in 2017, and the Ph.D. degree in computer engineering from Sejong University, Seoul, Republic of Korea, in 2023. From 2018 to 2020, he was a Researcher with the Agency for Defense Development (ADD), Republic of Korea. From 2021 to 2023, he was an Officer for cyber operations planning and cyber operations training at the Army Cyber Operations Center (ACOC). He currently conducts research at the Joint Forces Military University (JFMU), where he studies advancements in defense policy, military strategy, defense planning, and joint coalition operations. His research interests include cyber intelligence surveillance and reconnaissance (ISR) and cybersecurity.

DONGKYOO SHIN received the B.S. degree in computer science from Seoul National University, South Korea, in 1986, the M.S. degree in computer science from Illinois Institute of Technology, Chicago, IL, USA, in 1992, and the Ph.D. degree in computer science from Texas A&M University, College Station, TX, USA, in 1997. He is currently a Professor with the Department of Computer Engineering, Sejong University, South Korea. From 1986 to 1991, he was with Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he was a Principal Researcher with the Multimedia Research Institute, Hyundai Electronics Company, South Korea. His research interests include machine learning, ubiquitous computing, biosignal data processing, and information security.