IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 September 2023, accepted 9 October 2023, date of publication 16 October 2023, date of current version 19 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3324901

RESEARCH ARTICLE

Improved Cyber Defense Modeling Framework for Modeling and Simulating the Lifecycle of Cyber Defense Activities

DONGHWA KIM[1,2], MYUNG KIL AHN[1], SEONGKEE LEE[1], DONGHWAN LEE[1], (Member, IEEE), MOOSUNG PARK[1], AND DONGKYOO SHIN[2,3], (Member, IEEE)

[1]Cyber Technology Center, Agency for Defense Development, Seoul 05771, South Korea
[2]Department of Computer Engineering, Sejong University, Seoul 05006, South Korea
[3]Department of Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, South Korea

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

This work was supported by the Agency for Defense Development by the Korean Government under Grant 912921301.

ABSTRACT It is difficult to assess the business impact of a cyberattack and implement appropriate strategies or policies to enhance cyber resilience and counter future attacks. Penetration testing, which is currently gaining popularity, has been employed to assess cyber defense levels in actual operating environments. However, it is expensive and time-consuming and only reveals the current state of a problem without providing insights into potentially better alternative strategies. To overcome these limitations, cybersecurity modeling and simulation (M&S) research, which includes the crucial component of cyber-defense modeling, is being actively conducted. Most cyber defense modeling approaches only model defenses as a response to cyberattacks, neglecting to consider the complexities in the actual cyber defense activities of organizations. Consequently, the intended aim to evaluate and enhance cyber defense capabilities through analysis cannot be met. In this study, we present a cyber defense process model that models the entire lifecycle of cyber defense activities as the following five phases: prevention, monitoring and detection, initial response, attack analysis, and recovery response. This model not only accounts for defense steps that had been neglected in previous studies but also offers improvements to previously introduced defense steps. Additionally, we present a framework for applying initial and recovery response models by progressively integrating a unit response behavior model to counter cyberattacks. The applicability of the proposed model was verified by using a constructed prototype. The results of this study can be applied to developing an M&S-based experimental environment for assessing the sustainability of missions/businesses that have faced cyberattacks.

INDEX TERMS Cybersecurity modeling and simulation, cyber defense model, cyber defense process model.

I. INTRODUCTION

With the increased complexity and interconnectedness of society, more functions and data are being managed by personalized, privacy-rich devices such as smartphones and personal computers. Consequently, cyberattacks targeting these devices pose serious problems for individuals and businesses in modern society. These problems are comparable to those faced by the military in its operational environment [1], [2]. However, unlike the private sector, the defense sector attempts to avoid such vulnerabilities in weapon systems by treating isolated networks and distinct system environments as physically separate from the Internet. In the defense sectors of most nations, cyberattacks have rarely disrupted or disabled military operations, making it difficult for the military to envision the impact and repercussions of cyberattacks on operational missions. This makes it challenging to analyze potential problems from these attacks and adopt appropriate countermeasures against them.

There are numerous strategies for mitigating cyberattacks. One approach is to utilize a cybersecurity framework (CSF) [3], which provides the strategic perspective

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

and technical components essential to constructing an organization's comprehensive cybersecurity infrastructure. It is accompanied by a cybersecurity maturity model (CMM) [4] that assesses and categorizes these components in order to prioritize informed decision-making. Another approach entails conducting a thorough technical analysis of potential attack vectors within the organization's current security framework. This analysis entails evaluating the mission/business impact of potential attack scenarios and incorporating tactical enhancements to prepare for cyberattacks.

This work focuses on the second approach, which can be approached in two different methods. The first method, the penetration test, is conducted by numerous businesses on their actual network infrastructure to identify vulnerabilities and attack-susceptible surfaces and select more effective defensive systems. Even in the military sector, divisions frequently conduct penetration tests to share valuable information regarding newly learned lessons and potential ideas for improvements [5]. However, applying penetration testing to large-scale networks and systems is expensive in terms of cost, time, and personnel requirements, and the cost of multiple perspectives increases proportionally when testing is applied to a variety of attack scenarios. Therefore, penetration testing cannot be used to develop policies or procedures for cyber defense operations.

The second method involves conducting cybersecurity modeling and simulation (M&S) experiments [6], [7], [8], [9], [10], [11]. Although the fidelity of these experimental results may be lower than those obtained through penetration testing in a real environment, establishing the environment for these experiments is significantly more cost-, effort-, and time-efficient. Consequently, sufficient experimentation with various scenarios can provide the data required to determine the tactics/policies employed by an organization and the response it provides in the event of a cyberattack to maintain its mission or business continuity [10]. To address the fidelity of M&S results, research has also been conducted on developing a constructive-based M&S environment that is interoperable with live-virtual environments [12]. Numerous component technologies are necessary for developing proper M&S approaches for cybersecurity. Unlike cyberattack simulation technologies, cyber defense simulation technologies have not been extensively researched [13], [14]. Most organizations that implement cybersecurity M&S have robust cyberattack response teams and processes and follow government-mandated cyber incident response guidelines [6], [12], [15], [16]. However, current cyber defense modeling studies have not experimentally verified such approaches. This is because many cyber defense modeling studies [17] have been conducted as either ancillary studies aiming to verify the performance of cyberattack modeling instead of focusing on the entire defense activities of an organization or fragmented studies that only focus on individual defense devices.

To address this issue, we propose a cyber defense process model framework comprising five steps, namely prevention, monitoring and detection, initial response, attack analysis, and recovery response, based on an analysis of cyber incident response guidelines implemented by major advanced nations. This was done to implement the cyber defense activities in cybersecurity M&S as a complete cycle. Additionally, we defined the functions, procedures, and information flows for each step of the model. The first step in the model, the prevention step, involves modeling the function of security equipment and security software in a manner consistent with those of previous studies [9], [15], [17]. The next step, the monitoring and detection step, models the monitoring function of a security operation center (SOC) and the attack detection function. Regarding the response step, depending on the amount of information and the purpose of the response, it is modeled into the initial response step, which aims to avoid the spread of attacks, and the recovery response step, which aims to eliminate attacks and restore damaged or lost functions. An attack analysis model is added between the two models to model the time-consuming process of determining the information related to a cyberattack. The cyber defense process model and its detailed steps can be used to conduct simulations that include the general procedures and functions specified under cyber incident response guidelines and reflect various organizational policies, structures, and information-sharing systems. The performance of the proposed framework was confirmed using experiments with an implemented prototype. Additionally, we used the prototype to assess the impact of confidentiality and availability on the effectiveness of various defense policies against cyberattacks.

The results of this study can be used to determine the effectiveness of the current cyber-defense structure, policies, and processes of an organization in protecting mission/business-critical systems from various cyberattacks. Additionally, they can be used to identify measures to enhance the efficacy of existing cyber defense measures and provide a compelling rationale for prioritizing them. In the future, these results can be applied to an experimental environment to assess the impacts of cyberattacks on different missions/businesses.

The rest of this paper is organized as follows. Section II introduces major agency guidelines and related research on cyber defense modeling, and Section III describes the proposed cyber defense process model framework and comprehensive defense model. Then, Section IV describes the network and cyberattack considered in our experiments with the prototype, followed by the results and analysis of the experiments conducted with seven different configurations. Finally, Section V concludes the paper.

II. RELATED WORKS

A. CYBERSECURITY STANDARDS

1) CYBERSECURITY FRAMEWORK

The Cybersecurity Framework (CSF) [3] is a standard framework established by the U.S. National Institute of Standards and Technology (NIST) to provide a full-cycle

strategic direction and technical practices for proactively preventing cyberattacks. The five functions of "Identify," "Protect," "Detect," "Respond," and "Recover" defined in the Framework Core of the CSF are organized according to the life cycle stages for constructing a cybersecurity system, and the technical practices to be performed in each function are classified by category and subcategory. The CSF Implementation Tiers are intended to provide the context and methodology for implementing processes to address cybersecurity threats, as well as the level at which these processes are performed, ranging from Partial (Tier 1) to Adaptive (Tier 4).

A Cybersecurity Maturity Model (CMM) is a method for assessing an organization's implementation and operations of cybersecurity practices and identifying priority areas for improvement from a strategic perspective. The Cybersecurity Capacity Maturity Model (C2M2) [4], devised by the U.S. Department of Energy, is a model of the CMMs that examines and assesses over 300 action items in 10 domain areas and diagnoses them at three levels. In addition to CFS, the mapping relationship between CSF and C2M2 can be used to evaluate a CSF-based security environment.

The focus of this study is to validate, through engagement-level simulations, that cyber defense environments, systems, and processes developed using methodologies such as CSF and CMM function at the desired level against specific attacks. In comparison to the Framework Core of the CSF, the technical practices of Detect, Respond, and Recover can be tested to ensure they function in a timely manner during a specific attack. If they do not, it can analyze the reasons for their failure, including the temporal element.

2) CYBER INCIDENT RESPONSE FRAMEWORKS

Numerous nations have provided guidelines for both public and private sectors on cyberattack preparation, including the existing organizations and processes that can respond to cyber breaches [18], [19], [20], [21]. This section describes the steps in establishing a cyber-defense process and details each step. The working of numerous organizations with cyber defense manuals or SOCs are based on these guidelines.

Figure 1 summarizes the cyberattack response frameworks adopted by four major organizations. The basic steps include preparing for a potential attack, recognizing a cyberattack after detection, containing the spread of the attack and eradicating it, and restoring the system. Additionally, the organization employs postmortem analysis to implement measures for improving security.

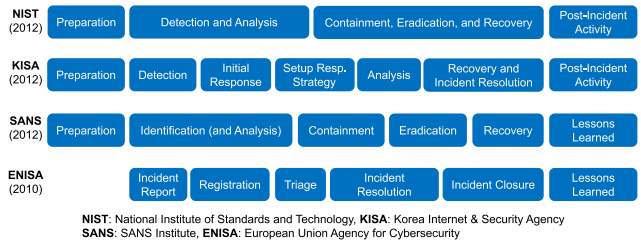


FIGURE 1. Computer security incidence response frameworks of major agencies for cyber security [18], [19], [20], [21].

Generally, the preparation step involves setting up the necessary components required to respond to an incident, such as establishing an emergency communication system, preparing the tools (both hardware and software) required for incident analysis, and preventing potential incidents by ensuring the proper security of systems, networks, and applications.

Each organization is similar in how it performs the following steps: detecting cyberattacks, understanding the context of a breach, preventing the spread of an attack, and undertaking attack analysis. However, each has distinct guidelines for recognizing and recovering from a breach. After the complete eradication of a cyberattack, the process of system normalization is initiated. After an organization has recovered from a breach, it reflects on the incident and undertakes preparations to create a more robust security system.

B. CYBER DEFENSE MODELING STUDIES

Kotenko et al. [7] proposed a framework for conducting M&S for cyberattack and defense, in which three types of agents operate in a distributed and cooperative manner: cyberattack, cyber defense, and user. They implemented it using a combination of discrete-simulation tools and packet-level simulators and presented the results of simulation experiments involving distributed denial of service attacks, which are significant issues. Defense agents, which are the primary focus of this research, are further classified according to their functions as follows: information processing (sampler), attack detection (detector), filtering and balancing (filter), and traceback and investigation (investigator). The sampler is a defense agent that learns data for hop-count filtering (HCF), source Internet Protocol (IP) address monitoring (SIPM), and bits per second (BPS) prior to the actual simulation. The agent responsible for attack detection is the detector, which detects attacks based on the threshold value derived from the sampler. When messages are detected by the detector, the filter blocks them. The IP address of the attack source is deduced from the malicious packets and further traffic from that address is blocked.

Ten et al. [8] proposed and experimentally validated a real-time monitoring, anomaly detection, impact analysis, and mitigation strategy (RAIM)-based supervisory control and data acquisition (SCADA) security framework and evaluation method for power systems. Implementing the RAIM framework can effectively mitigate the impact of a cyberattack on a power system. Methods for modeling and assessing the impact of cyberattacks have also been presented for this purpose. The first step in RAIM involves the real-time monitoring of information and power systems, which is followed by anomaly detection step, wherein the spatial, temporal, or spatio-temporal correlations between observed events are analyzed to detect cyberattacks and

generate possible cyberattack scenarios. Then, in the impact analysis step, the vulnerability of information and power systems to cyberattacks is evaluated based on the behavior of the perpetrator and possible attack scenarios, and the probability of capacity loss in the power system due to this vulnerability is evaluated. Finally, in the mitigation strategy, appropriate control actions are taken to prevent and mitigate risks based on the progression of the attack and risk situation in each of the three stages (attack attempt, ongoing attack, and ongoing attack targeting the power system).

Cho et al. [9] proposed a method for integrating three defense methods, namely the intrusion detection system (IDS), deception, and moving target defense, using an integrated modeling approach. The proposed method was implemented using stochastic Petri nets, and the performance of the three defense methods in combination was experimentally validated using evaluation metrics, such as system lifetime, accumulated defense cost, attack success probability, and accumulated attack cost.

Rajivan et al. [22] proposed a method for simulating a cyber defense team of analysts with the aim of comprehending team performance from both a macro perspective, which involves team effectiveness, and a micro perspective, which involves the collaboration between the analysts in a team. They thoroughly outlined the steps in modeling the number of analysts in a team and the manner wherein they should collaborate to effectively manage many security alerts. They presented a comprehensive approach to human modeling, which included learning strategies for individual analysts to attain greater rewards and collaboration strategies for teams to enhance performance. Overall, the model for cyber defense activities is limited to managing security notifications, resulting in the simulations being limited to tasks such as selecting the analysts for a team and determining their cooperative strategy for handling more alerts.

Analyzing Mission Impacts of Cyber Actions (AMICA) [10] is a multi-layered M&S approach for quantitatively assessing the operational mission impact of a cyberattack on a specific mission, which includes operational (kinetic) missions, mission-related computing infrastructure, cyberattacker tactics, techniques, and procedures (TTPs), and cyber defender TTPs. The working of a cyber defense model includes the following steps: the triage step, which identifies and classifies security alerts, including attack detection, which generates security alerts; the forensics step, which analyzes the target of security alerts; and the reboot, restore, and rebuild steps, which are performed according to the recovery actions required after the previous step. Excepting the activities in the triage step, those in the forensics and recovery activity steps are simulated in terms of time, spanning from 5 min for straightforward actions, such as rebooting, to 6 h for identifying infected hosts using derived signatures.

The response guidelines for cyberattacks can be analyzed based on the preceding information as follows.

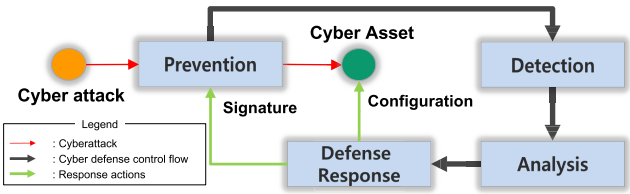


FIGURE 2. Generalized cyber defense modeling architecture in existing research.

(i) In the preparation step, attempts are made to prevent as many cyberattacks as possible before they are even recognized. (ii) In the operational process, attacks are detected rapidly and accurately. (iii) Following cyberattack detection, an initial response to mitigate the damage and contain its spread is implemented. (iv) Subsequently, an attack analysis is conducted to understand the precise circumstances and details of the attack. (v) Efforts are continued to completely eradicate cyberattacks in the organization and restore the normal operation of mission/business-critical systems based on the information obtained, such as the tools used in the attack, the method of the attack, and the scope of the attack. (vi) Once the systems are stabilized, the steps in cyber defense are iterated, and preparations are started for dealing with new attacks and detecting any attempted attacks.

In contrast, generalized architecture of previous cyber defense modeling studies in cybersecurity M&S primarily included prevention and response models, as depicted in Figure 2, that could not accurately represent practical cyber defense activities [9], [15], [17], [22], [23], [24]. There are parts of the cyber defense process that can have important consequences but are not simulated in previous studies. Examples include how to handle misuse by legitimate users that is ignored by the security control center, and the critical initial response after detection of a cyberattack. Even if there was an investigation or analysis phase [7], [8], [10], it was limited to information output with either only the time delay or no consideration for policy changes, resulting in an environment unsuitable for conducting a variety of defense-related experiments.

III. CYBER DEFENSE PROCESS MODEL

Based on the analysis presented in the previous section, we developed a framework for a cyber defense process model that comprised five steps, as depicted in Figure 3, to implement the entire lifecycle of cyber defense activities in cybersecurity M&S. Figure 3 illustrates the flow of controls, information, and defensive actions required to model cyber defense activities conducted at each step. The modeling approach for the five comprehensive defense models of the cyber-defense process is detailed below.

A. PREVENTION MODEL

The prevention model primarily uses security equipment and security software, such as a firewall, an intrusion

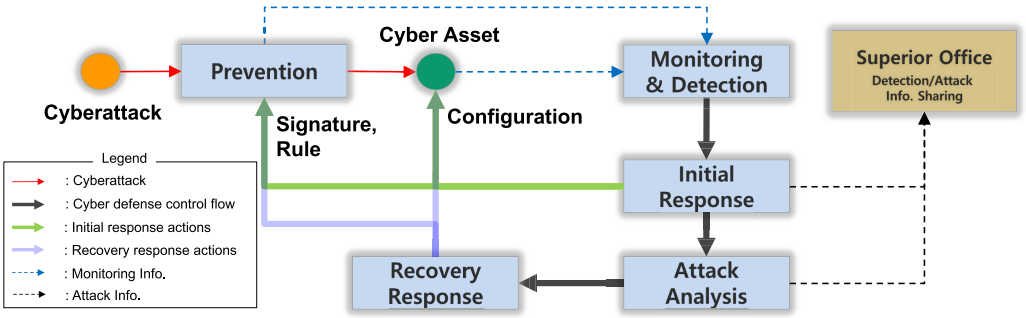


FIGURE 3. Architecture of the proposed cyber defense process model.

prevention system (IPS), an antivirus, and endpoint detection and response (EDR). In most organizations, these tools are deployed at key network locations or on each host to prevent cyberattacks, and they play a role in proactively preventing known cyberattacks. Functionally, they continually monitor the network traffic, files, and processes externally entering a network or computer system to detect and block known cyberattacks with signatures or detection rules.

The prevention model has frequently been employed as a defense model [15]; its general operational concept is depicted in Figure 4. If a file or process in the cyber-asset model or traffic in the network model has an identifier registered as a signature, it is detected as an attack; otherwise, it is permitted to pass. If a signature is detected, the object (traffic, file, process) is blocked, and security alerts and attack information are transmitted to the monitoring server (e.g., Security Information and Event Management (SIEM) server, which is a monitoring and detection model).

Like in previous studies, a prevention model, which is applicable to network-based security devices such as IDS/IPS and firewalls and host-based security software such as antivirus and EDR, was applied in the current study. If it is necessary to simulate threats to security caused by mobile devices or bring-your-own-device (BYOD), the model for mobile device management (MDM) software adopted by each organization can be used as one of the new prevention models. Behavior-based and threat TTP-based detection were incorporated into this model, distinguishing it from the

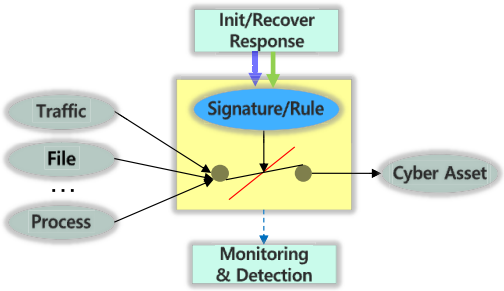


FIGURE 4. Prevention model.

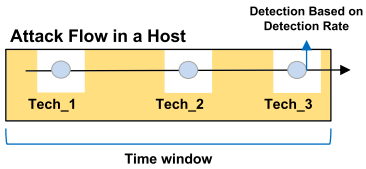


FIGURE 5. Detection based on threat intelligence.

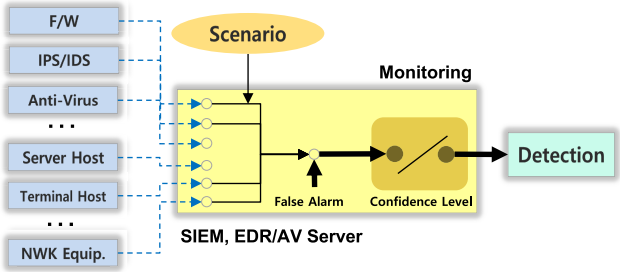


FIGURE 6. Monitoring and detection model.

pre-existing model, which focused on signature detection. Figure5 illustrates the concept of a threat TTP-based detection simulation, where a detection rule detects consecutive occurrences of specified attack techniques during a specified time window. This concept enables the proposed process model to simulate the mechanisms of Cyber Threat Intelligent (CTI) sharing frameworks.

The monitored objects (traffic, files, processes) and attributes such as signatures or detection rules and detection rates for each model device (IPS, antivirus) were the inputs to the prevention model. In the initial configuration, the input is provided and then iteratively updated by the initial response/recovery response model throughout the simulation process.

B. MONITORING AND DETECTION MODEL

The monitoring and detection model represents the SOC of an organization and reflects that security devices and programs in real-world scenarios are recognized differently based on monitoring status, reporting period, and level of confidence; Figure 6 illustrates the conceptual structure of this model.

Monitoring and detection of attacks are performed in the detailed security device model of the Prevention model, but monitoring at the SOC of the security device and handling of security alarms generated by the security device based on their reliability are handled in the Monitoring and Detection model. In a typical Internet environment, most security systems are periodically monitored and updated. However, in the case of an isolated network, such as an industrial control system or a defense weapon system, security software is frequently not implemented. In case it is, it cannot be centrally monitored and updated owing to the performance limitations of legacy systems. To account for these practical conditions, it is necessary to establish a monitoring status and reporting period for each security system. Moreover, even if security alerts occur, they may be ignored because of frequent false-positive security alarms (especially network-related alarms) and unintentional security violations by normal users. Therefore, it is necessary to reflect the confidence level [25] of each security system.

Monitoring server apparatus models can be represented by enterprise security manager (ESM)/SIEM servers, EDR servers, and antivirus servers with monitoring functionality. Antivirus and EDR servers can monitor the security software of each end host, while the ESM/SIEM can monitor servers and network security equipment. The monitoring entities in the monitoring and detection model are security hardware or software employed in the prevention model.

During the scenario authoring process, the connection of the monitored entity to the monitoring server, monitoring period, false detection rate, and confidence level are entered as inputs to the monitoring and detection model. Once the monitoring entity is configured to communicate with the monitoring server, it transmits the simulated monitoring traffic to the server. Here, traffic monitoring should include information regarding the presence/absence of a cyberattack and the detection/non-detection of such an attack; if a cyberattack occurs, details about the attack should be included. Detected cyberattack information is utilized in the initial response step, whereas undetected cyberattack information is extracted from the attack analysis model as attack information based on probability. Attack information unidentified during the defense activities is only used for statistical analysis after the conclusion of the simulation.

Installed security software will not send monitoring traffic to the server if it is disconnected from it. In this case, if a cyberattack is identified through a signature, it will be blocked, but the organization will not take additional defensive measures such as implementing the initial response step. Additionally, it will incur additional costs to update signatures and detection rules. Based on the confidence level, the monitoring server determines whether to trust the cyberattack alarm when it receives it. For instance, if an antivirus signature with a confidence level of 100% detects and monitors a cyberattack, processes such as initial response and attack analysis are sequentially carried out. However, if a cyberattack is detected based on an EDR rule with a confidence level of 70%, the attack alarm is determined to have a 70% probability based on the confidence level, and the aforementioned processes are implemented. Otherwise, the attack alarm is ignored with a 30% probability.

C. ATTACK ANALYSIS MODEL

After a cyberattack is identified, the attack analysis model discovers other compromised cyber assets and identifies information related to the attack (signatures, detection rules). Depending on the number of available security staff, their skills, and the size of the network to be analyzed, attack analysis can be quite time-consuming in real-world. Consequently, it is essential that each organization employs distinct strategic approaches. An organization should be able to decide whether it wants to quickly conduct an attack analysis and recover the mission/business even if the results are incomplete or take a longer and more careful approach and strive to completely eradicate the attack.

Figure 7 presents a conceptual illustration of the factors that can influence the attack analysis process and the resulting model with time delays. The attack analysis model receives the number of analysts capable of performing the analysis, expertise level of each analyst, size of the network to be analyzed, and required accuracy of the results as inputs. The model calculates the time required for attack analysis based on the input data. After the calculated time delay, it sends the list of infected hosts, attack method for each host, and mission/business impact to the recovery response model, which performs the next step.

The required accuracy is policy setting that specifies the amount of data to be extracted during attack analysis. This setting determines whether the analysis is time-consuming but highly accurate or fast but less accurate. For instance, if 90% of the required accuracy is simulated, 10% of the infected hosts will be absent from the resulting host list of the attack analysis model. With the required accuracy of 60%, a list that is missing 40% of the hosts will be received. The other outcomes, including those with the attack signatures, will be identical.

The duration of an analysis is determined by the number and proficiency levels of analysts. When authoring a simulation scenario, the number of available analysts and their skill levels are specified, with the skill levels being expressed as high, medium, or low. Using data collected during analyst education or training courses, the analysis time can be calculated based on the number of individuals and their skills. The data from a hands-on training course conducted as part of an education/training process can be modeled as a function using statistical analysis or constructed into a database and applied to the simulation. For example, the skilled level can be simulated to affect the analysis time by multiplying the ''high'' level by 0.5 or the ''low'' level by 2, with the ''medium'' level as the base (scale factor 1). If the analysis is performed by a team, and the effects of diverse team members and their cooperation need to be simulated, the methodology proposed by Rajivan et al. [22] can be used.

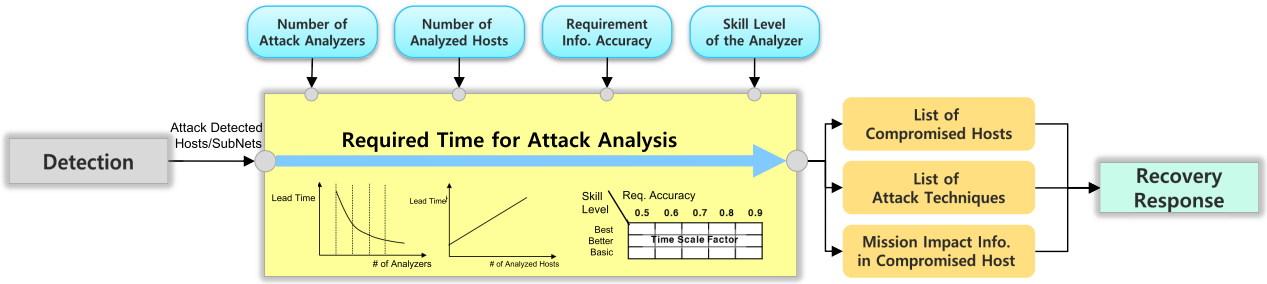


FIGURE 7. Attack analysis model.

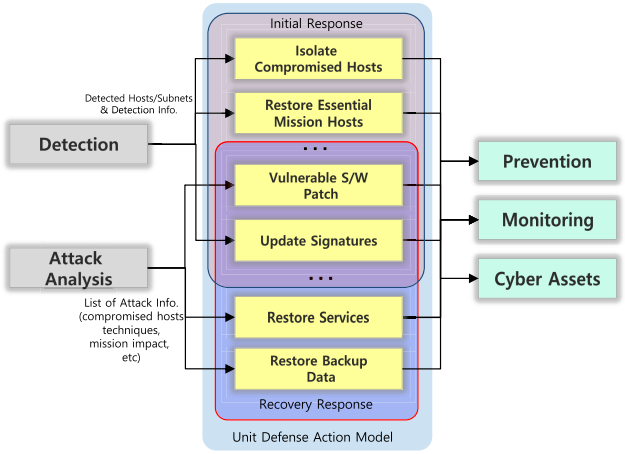


FIGURE 8. Initial response / Recovery response model.

Using data from education/training courses, the relationship between the required accuracy and analysis time can be derived. This can be determined through statistical analysis using data on the time required to find 50, 70, and 90% of the attack information.

The size of the network to be analyzed also significantly impacts the analysis duration. It refers to the size of network hosts managed by each organization/department to be simulated and potentially reflects the time required to analyze servers and PC terminals differently; however, generally, the network size and time required for attack analysis are proportional. Correlations can also be determined using information gathered during education/training programs.

We inferred that the hosts covered by the analysis would differ based on the policy of an organization regarding whether the analysis should be performed only for the department where the attack was detected or for the entire organization. This affects the time required to conduct attack analysis.

D. INITIAL RESPONSE/RECOVERY RESPONSE MODEL

The initial response refers to the series of actions performed by an organization promptly after identifying a cyberattack to stop its spread and prevent further damage in accordance with its specified incident response manual. For instance, if a cyberattack is detected on a PC, the response team may disconnect the PC from the network, turn off the power, and analyze the attack. Similarly, if an attack is detected on a server, the response team can quickly replace the server with a redundant one to maintain services while analyzing the attacked server. Recovery response refers to the process of acting to completely eradicate cyberattacks within an organization using the attack information obtained from the attack analysis step as well as restoring damaged functions related to essential missions or services.

The response step in this study has been modeled in two distinct time frames, with an initial response model to limit the spread of attacks and damage immediately after cyberattack detection and a recovery response model for attack elimination and system restoration after conducting attack analysis. The detailed actions of the initial and recovery response steps are selected from a set of previously constructed unit defense behavior models. The steps can be developed as a framework for a unit defense behavior model set, such that users can readily incorporate the unit defense behavior models required for simulations. If the required unit defense behavior model is already included in the set, it can be used directly; otherwise, it can be implemented, enabling the progressive accumulation of the set. When authoring the simulation scenario, the actions for the initial response/recovery response steps are chosen from the set of unit defense behaviors by checking the manual of the organization. Additionally, the available budget, time period, and manpower of the organization are depicted as the available costs; only the unit defense actions within the available cost constraints are selected and implemented. The operational concept of the initial response model and the recovery response model is depicted in Figure 8. In Figure 8, the initial response model executes unit defense actions chosen based on the results of the detection step through the prevention model, monitoring model, and cyber asset model. Likewise, the recovery response model executes unit defense actions chosen based on the results of the attack analysis step through the prevention model, monitoring model, and cyber asset model.

While the initial and recovery response models share several functional similarities, there are distinctions in the information obtained during the simulation process and the

possible individual unit defense actions. The following are examples of unit defense behaviors that can be modeled as either specific to each model or common to both:

- Adding IP blocking/monitoring to Prevention models such as IPSs/Firewalls/Anti-Viruses
- Isolating an attacked host from the network
- Restoring the functionality of an attacked host to its state before an attack
- Restoring deleted host data from a backup
- Updating vulnerable applications on infected hosts to their most recent versions
- Registering the code signature of an attack with the prevention model

Unit defense behavior models associated with cyber assets or attack models can be defined and modeled in numerous ways using simulations from previous studies on cyber-defense models. For instance, unit defense behaviors can be modeled using the defense techniques outlined in the "Mitigations" component of MITRE ATT&CK® [16] or D3FEND™ [26]. [1]

The defense behavior of each unit can be modeled separately as needed but should include the following data.

- Input information required to execute unit defense actions (e.g., IP address, attack signature, target host, and other attack model-dependent information)
- Applied model (the type of prevention model e.g., antivirus, firewall; the type can be selected multiple times)
- Information regarding whether it can be executed using an initial response model, a recovery response model, or both.
- Cost of execution
- Policy attributes (mission/service preservation or removal/blocking of cyberattacks)

The policy attribute specifies whether the unit defense behavior is mission-related (to restore/maintain missions/services) or defense-related (to prevent/eliminate cyberattacks). This can be applied to developing a countermeasure recommendation algorithm that prioritizes the execution order of unit defense behaviors to maintain missions/services or stop or eliminate cyberattacks within the available cost constraints.

The initial response model and attack analysis model can share information with other organizations regarding cyberattacks. Receiving shared detections of attacks from the initial response model raises the cyber readiness of an organization. This can be accomplished by lowering prevention model thresholds to increase detection rates or by increasing confidence levels so that even minor security alerts may trigger post-detection activities.

Organizations that have shared cyberattack data that has been analyzed by the attack analysis model can add threat intelligence as an attack detection mechanism to the prevention model. This enables organizations that have not yet been attacked to proactively block attacks from the same attacker or to detect attacks that have already occurred but were not detected proactively. This feature can be used to simulate threat information sharing facilities that are being constructed to prevent the same attack from spreading to other organizations.

[1]The MITRE ATT&CK and D3FEND are classification models for the tactics and techniques used by cyber attackers and defenders, which are based on the analysis of real-world attack cases and cyber defense activities.

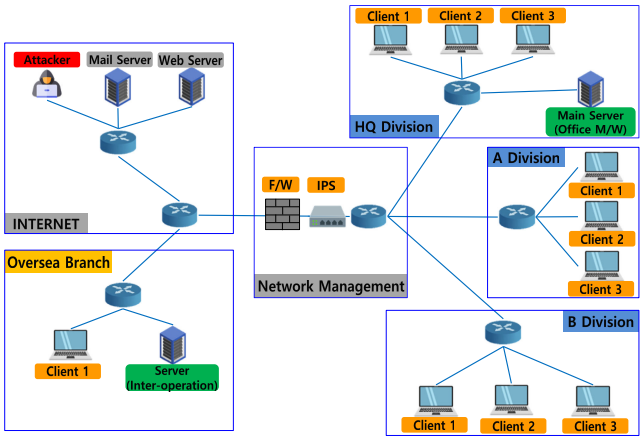


FIGURE 9. Network topology and composition of target organization.

IV. EXPERIMENTAL VERIFICATION

We verified the functionality of M&S by implementing prototypes of the cyber defense process model and detailed models for each step, as described in Section III. To ensure that the simulated behavior of each implemented model functioned as intended, the attack was restricted to one scenario. We also diversified the defense policies and configurations of the test organization across 14 cases in seven experimental scenarios to determine their impact on the attack success probability and mission/business availability. The simulation engine vsTASKER [27], which is a general-purpose discrete event simulation tool, was used for this implementation.

A cyberattack is primarily performed to exfiltrate data from central missions/business servers. Defense activities mainly aim to prevent (information leakage) attacks and maintain central server availability. Assuming that the cyberattack is an advanced attack that exploits zero-day vulnerabilities and cannot be detected or blocked by the prevention model, a security alarm is expected to only be activated in the event of a large-scale information leak. Figure 9 shows the network and host configurations used in the experiments. To build the necessary cyber space environment for the experiments, a cyber asset model, network/communication model, service model, and cyberattack model for cyberattacks were implemented.

A. CYBER ATTACK SCENARIO

The cyberattack was designed using techniques from the MITRE ATT&CK® framework [16]. Figure 10 depicts the overall attack flow; Figure 14 in the Appendix depicts the attack sequence in greater detail. Cyberattacks employ twelve

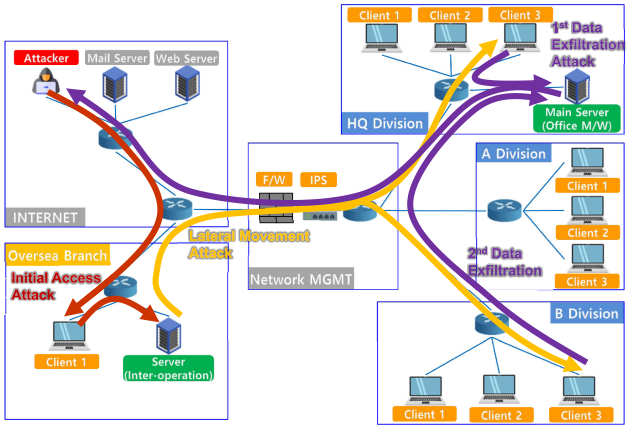


FIGURE 10. Brief cyberattack on the target network.

distinct techniques. In Figure 10 and 14, the attack by HQ_Client3 on HQ_M/W_Svr, the main mission/business server, is the 1st attack wave. If the 1st attack wave fails, the 2nd attack wave is executed by B_Div_Client3.

The cyberattack was carried out to exfiltrate sensitive data from HQ_M/W_Svr, which is a mission/business main server configured with Office middleware. The 1st wave consisted of 18 attack techniques while the 2nd wave consisted of four additional attack techniques.

B. CYBER DEFENSE SCENARIOS

Cyber defense scenarios were included in each simulation case to verify the effectiveness of each defense step executed in accordance with the cyber defense process model, which is based on behavioral detection rather than the previously studied detection/blocking method using security equipment.

1) DEFAULT DEFENSE CONFIGURATION

The default configurations of each defense step are listed in Table 1 for comparison purposes. In each case, the default values were used for the defense parameters that had not been explicitly mentioned in the experiments. The duration of each step depended on the actual response time to the security breach [28]. Specifically, the average time for attack analysis in [28] was assigned to the time required by the attack analysis model in the default defense configuration because simulation-required education/training practice data had not yet been developed. Additionally, the required accuracy reflected the tendency of the required time to increase exponentially with the accuracy, and the required time for the network size was proportional to the size of the host.

2) TEST DEFENSE CONFIGURATIONS

To test the effect of various cyber defense attributes on availability and confidentiality, the cyber defense was configured as shown in Table 2. The scenario numbers for the comparison of each defense attribute are also shown.

TABLE 1. Default defense configurations for the experiments.

Defense Step	Configuration Item	Value
Monitoring & Detection	Confidence Level in HQ_M/W_Svr	50%
	Installation Anti-Virus in B_Div	None
Initial Response	Initial Response Completion Time	5 h
	Initial Response Unit Defense Action	Isolating Hosts, Registering IP/Signature
Attack Analysis	People & Skill level	10 hours
	Required Accuracy	50%
	Network Host Size	Detected Division (15 hours required)
Recovery Response	Recovery Response Completion time	5 h
	Recovery Range	Detected Division (15 h required)
	Recovery Response Unit Defense Actions	Registering IP/Signature, Host System Recovery, Host Data Recovery

TABLE 2. Defense configurations for the policy variations in the defense steps.

Defense Step	Configuration Item	Configuration Value	Scen. Num.
Monitoring & Detection	Confidence Level	75%	(1)
		25%	
Attack Analysis	Required Accuracy	75% (15 h required)	(2)
		90% (30 h required)	
	Analysis Range	All Divisions (30 h required)	(3)

The confidence level refers to the probability of deciding whether to trust a security alert containing numerous false positives in the monitoring and detection step and continue with the planned defense activities. The experimental scenarios (1), (2), and (3) assumed that only the 1st wave of attack had been launched against HQ_M/W_Svr via HQ_Client3.

Advanced cyberattacks are characterized by persistent attacks, meaning that even if the 1st attack fails, there is a risk of a 2nd attack if the recovery response fails to completely eradicate the threat. To simulate such situations, we experimented with an additional attack scenario in which the first attack failed and the attacker reattempted an attack via a different network-connected host (B_Div_Client3). This attack scenario was tested on the host (B_Div_Client3) in two scenarios, namely one wherein no antivirus software had been installed and one wherein antivirus software had been deployed and monitored on the same host.

Additionally, two cases were simulated: a case wherein the same attack code had been used in the following attack and one wherein the attacker had realized that the attack had been detected and a different attack code has been used to evade detection. Table 3 lists the experimental configurations of the reattack scenarios. All the configuration items that had not been specified in each scenario were identical to the default defense configuration items.

TABLE 3. Defense configurations for re-attack scenarios.

Attack Code	Defense Step	Configuration Item	Configuration Value	Scen. Num.
Same Attack Code	Monitoring & Detection	Anti-Virus in B_Div	None	(4)
	Attack Analysis	Analysis Range	Detected Division (10 h required)	
			All Divisions (30 h required)	
	Monitoring & Detection	Anti-Virus in B_Div	Installed	(5)
	Attack Analysis	Analysis Range	Detected Division (10 h required)	
			All Divisions (30 h required)	
Different Attack Code	Monitoring & Detection	Anti-Virus in B_Div	None	(6)
	Attack Analysis	Analysis Range	Detected Division (10 h required)	
			All Divisions (30 h required)	
	Monitoring & Detection	Anti-Virus in B_Div	Installed	(7)
	Attack Analysis	Analysis Range	Detected Division (10 h required)	
			All Divisions (30 h required)	

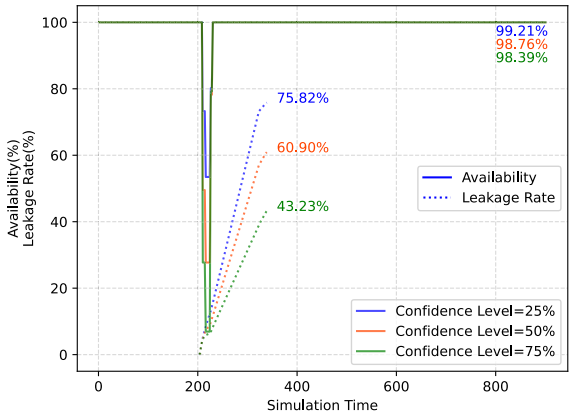
C. EXPERIMENTAL RESULTS

Figures 11, 12, and 13 graphically depict the experimental results for the seven scenarios. The graphs show the results for the data leakage rate (dashed line) on the core middleware server owing to cyberattacks and the availability of the same server owing to cyber defense activities (solid line), both as a function of the simulation time. Each graph represents the arithmetic mean of the data leakage rate and availability over 100 iterations of simulation time for each case. For instance, a leakage rate of 75.82% at the end of a cyberattack indicated that the attacker had shown a 75.82% probability of successfully exfiltrating the data, and an availability rate of 30% during the simulation indicated that there was a 70% probability that the server would be down at that time.

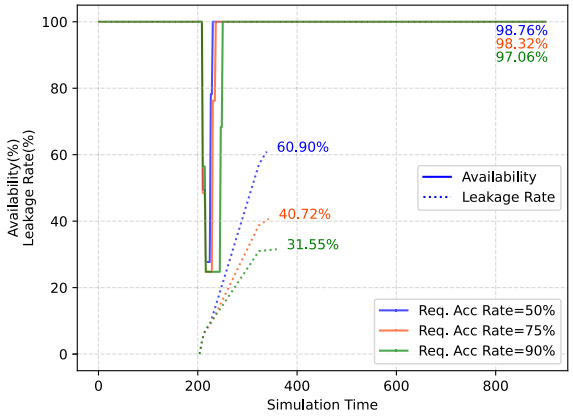
Figure 11 illustrates the experimental results when there were changes in (a) the confidence level in the monitoring and detection step, (b) the required accuracy in the attack analysis step, and the (c) range in the attack analysis/recovery response step when there had only been a first-time attack in the default defense configuration.

In every scenario, there was a tradeoff between the leakage rate and availability; when no cyberattack had been detected, data continued to leak while the server remained operational. By contrast, if a cyberattack had been detected, the server was considered inactive by subsequent defense activities such as the initial response/attack analysis step.

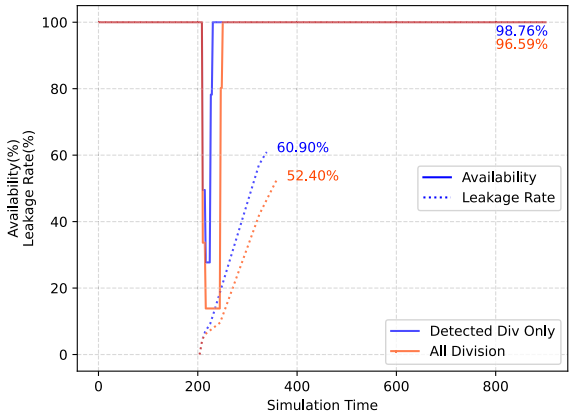
Experiments with the prototype demonstrated that the proposed cyber defense process model could be used to simulate the defense status of an organization more accurately by combining a wider variety of factors. Additionally, the model could be used to create optimal cyber defense policies capable of mitigating the impact of attacks while meeting the availability and confidentiality requirements of an organization.



(a) Different **confidence levels** at Monitoring & Detection step



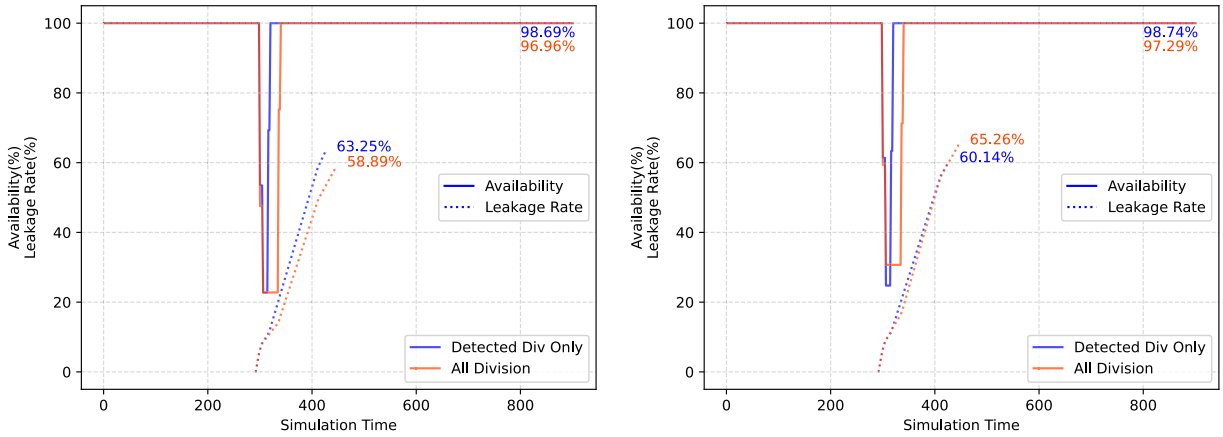
(b) Different **required accuracy rates** at Attack Analysis step



(c) Different analysis/recovery **ranges**

FIGURE 11. Availability and leakage rate results under the 1st attack (scenarios 1, 2, 3).

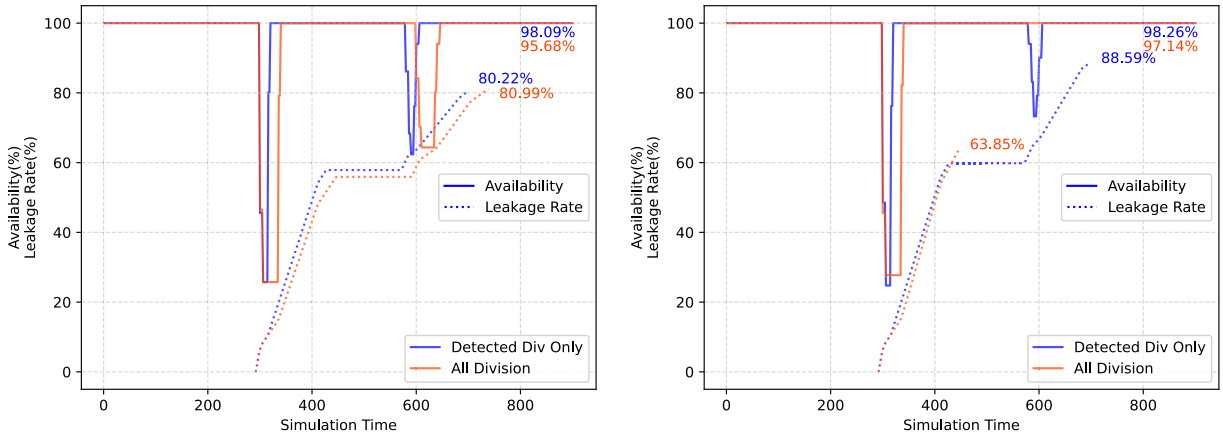
The leakage rate and availability results in experiments when an attacker reattacked an organization after the end of a cycle in the cyber-defense process model following the first attack are shown in Figures 12 and 13. Figure 12 depicts a scenario in which the second attack employed



(a) Different analysis/recovery ranges when A/V **is not installed** at B_Div

(b) Different analysis/recovery ranges when A/V **is installed** at B_Div

FIGURE 12. Availability and leakage rate results when the re-attack shared the same attack code as that of the attack (scenarios 4 and 5).



(a) Different analysis/recovery ranges when A/V **is not installed** at B_Div

(b) Different analysis/recovery ranges when A/V **is installed** at B_Div

FIGURE 13. Availability and leakage rate results when the re-attack had a different attack code from that of the attack (scenarios 6 and 7).

the same attack code as the first, and Figure 13 depicts a scenario in which a different attack code was used. The host (B_Div_Client_3) that functioned as the pivot for the second attack was compared in both scenarios (a) without antivirus software and (b) with antivirus software. Each scenario differed depending on whether the second attack pivot host (B_Div_Client_3) had been included in the defense activities (attack analysis/recovery response step).

When the re-attack utilized the same attack code, similar results were obtained, as shown in Figure 12 (a) and (b). This was attributed to taking preventative measures against attacks by registering signatures on both security devices and software in the recovery response step, based on the results of the attack analysis step when the first attack had been detected.

However, if a different attack code was employed in the second attack, as depicted in Figure 13, the results differed significantly from those in the previous cases. In the second attack, if no antivirus software had been installed on the pivot host (B_Div_Client_3), the information breach was not prevented, and availability was reduced, as shown in Figure 13 (a), while if antivirus software had been installed on the pivot host, and defense activities had been conducted at all sites, a second attack was prevented, as shown in Figure 13 (b). Consequently, then the availability of data would be maintained, and the risk of information leakage would be reduced.

Experiments on the second attack demonstrated that it was possible to simulate the entire cycle of cyber-defense activities using the cyber-defense process model, including security-enhancing activities, prior to the next attack.

TABLE 4. Comparison between the cybersecurity defense modeling features.

Defense Phase	Modeling Features	Cybersecurity Defense Modeling Approaches			
		Kotenko et. al. [7]	RAIM [8]	AMICA [10]	Proposed
Prevention	Procedure	✓	✓	✓	✓
	Network-based	✓		✓	✓
	Host-based			✓	✓
Monitoring & Detection	Procedure	✓	✓	✓	✓
	Detection	✓	✓	✓	✓
	Incident Report			✓	✓
	Sensitivity				✓
	False Detection				✓
Initial Response	Procedure				✓
	Triage			✓	✓
	Contain-ment				✓
	Range				✓
Attack Analysis	Procedure	✓	✓	✓	✓
	Req. Time			✓	✓
	Analysis Accuracy				✓
Recovery Response	Procedure	✓	✓	✓	✓
	Eradication	✓	✓		✓
	Recovery			✓	✓
Post-Incident Activity	Procedure				✓
	Information Sharing				✓

Additionally, these experiments demonstrated that optimal countermeasures could be devised by analyzing the parts that were potentially vulnerable to various attacks and evaluating the defense posture.

D. COMPARISON OF PROPOSED AND EXISTING APPROACHES

Table 4 compares the proposed method to the existing cyber defense modeling methods described in Section II-B. The comparison is made with respect to the standard guidelines specified in Section II-A2 and published by regulatory authorities in key countries. In the absence of performance criteria for evaluating the fidelity of simulated cyber defense activities, we employ a method that evaluates the extent to which these activities are consistent with the processes, capabilities, and security policy concerns outlined in established standards.

Most approaches supported both prevention and recovery response steps, with all of them supporting only the detection function of the monitoring and detection step, with the exception of AMICA [10]; the proposed model supported the incident report function. Some approaches included response action as the initial response step, but none included any systematic procedures; only fragmentary actions had been included. Regarding the attack analysis step, no approaches included incremental procedures or defense policies; the approaches included fragmented procedures without any consideration for defense policies.

No previous approach supported the inclusion of the post-incident activity step since it had assumed a singular attack. The proposed model was designed to execute defense activities in the recovery response step and return to the prevention step after information sharing, and the experiment verified the results of post-incident activities for secondary attacks. Consequently, compared to previous approaches, the proposed model was the only one that included all the guided procedures in Section II-A2 and could reflect the defense policy at every step.

V. CONCLUSION

The cyber defense process model and detailed defense models proposed in this study are more detailed and more freely reflect the defense activities that an organization is preparing or planning in response to cyberattacks in cybersecurity M&S. The result of this study is applicable to check preparing of responsibilities against cyberattacks, identify their problems, and improve their technical procedure and cybersecurity policy. Existing studies are limited to simulating cyber security systems and responses to attacks. In contrast, the results from the proposed study can verify and supplement the capabilities of the settings, organizational operations, information-sharing methods, policy establishment techniques, and response measures of each system for each defense step performed throughout the entire cycle of cyber defense activities. The results were validated using a prototype, which revealed that the proposed model could provide significant insights into effectively defending against cyberattacks. Nevertheless, within the framework of ongoing discussions regarding emerging cyber defense paradigms and approaches, such as cyber resilience, it is important to recognize the potential constraints linked to the proposed approach, which heavily depends on static procedures. Therefore, it is important to acknowledge the necessity for a more flexible integration of defense process models, enabling an agile simulation of anticipated defense activities in the near future, thereby expediting an evaluation of the cyber defense system. This study can be used to build an experimental environment for assessing the mission/business impact of future cyberattacks, as the simulation can be performed by easily changing the technical settings related to cyber defense.; this experimental environment can also be potentially used to test cyber resilience. In the future, we intend to examine a structure capable of representing cyber defense steps in a flexible and parallel manner and add more unit defense behavior models so that organizations can easily reflect on the practicality of their cyber incident response manuals.

APPENDIX
SEQUENCE OF STEPS IN A CYBERATTACK SCENARIO IN AN EXPERIMENTAL NETWORK ENVIRONMENT

Figure 14 depicts the detailed sequence of cyberattacks used in the experiments along with a flowchart representation of the attacking and targeted hosts.

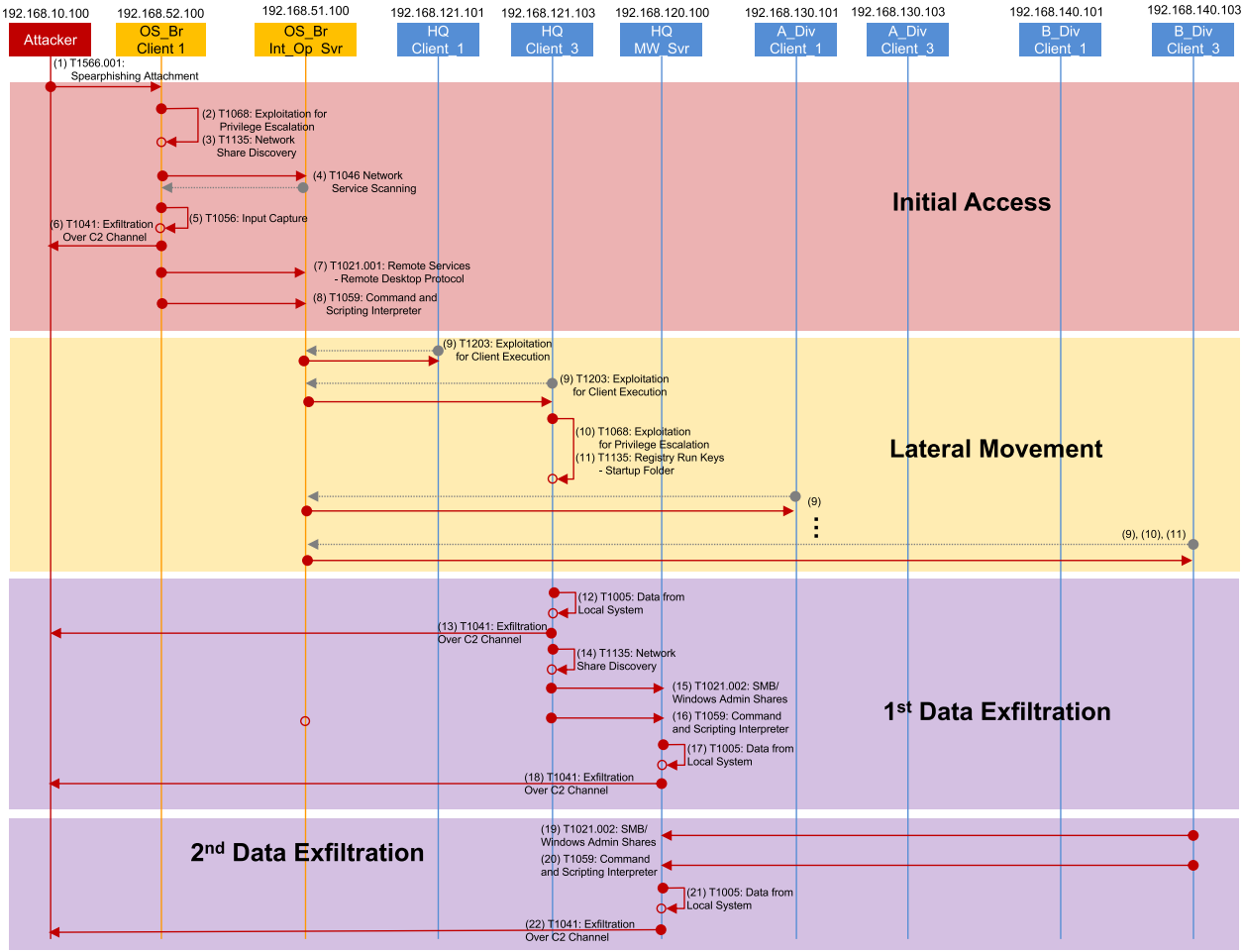


FIGURE 14. Overall flow of steps in a scenario wherein a cyberattack is targeting a network.

REFERENCES

[1] R. Koch and M. Golling, "Weapons systems and cyber security—A challenging union," in *Proc. 8th Int. Conf. Cyber Conflict (CyCon)*, May 2016, pp. 191–203.

[2] D. L. Bergin, "Cyber-attack and defense simulation framework," *J. Defense Model. Simul., Appl., Methodol., Technol.*, vol. 12, no. 4, pp. 383–392, Oct. 2015.

[3] *Cybersecurity Framework (CSF)*. National Institute of Standards and Technology. Accessed: Sep. 8, 2023. [Online]. Available: https://www.nist.gov/cyberframework

[4] *Cybersecurity Capacity Maturity Model (C2M2)*. USA Office of Cybersecurity, Energy Security, and Emergency Response. Accessed: Sep. 8, 2023. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[5] N. J. Hwang and K. B. Bush, "Operational exercise integration recommendations for DoD cyber ranges," Lincoln Lab., Lexington, MA, USA, Tech. Rep. 1187, 2015.

[6] M. K. Ahn, Y. H. Kim, and J. R. Lee, "Hierarchical multi-stage cyber attack scenario modeling based on G&E model for cyber risk simulation analysis," *Appl. Sci.*, vol. 10, no. 4, p. 1426, 2020.

[7] I. Kotenko, "Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security," in *Proc. 4th IEEE Workshop Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl.*, Sep. 2007, pp. 614–619.

[8] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[9] J. H. Cho and N. Ben-Asher, "Cyber defense in breadth: Modeling and analysis of integrated defense systems," *J. Defense Model. Simul.*, vol. 15, no. 2, pp. 147–160, 2018.

[10] S. Noel, J. Ludwig, P. Jain, D. Johnson, R. K. Thomas, J. McFarland, B. King, S. Webster, and B. Tello, "Analyzing mission impacts of cyber actions (AMICA)," in *Proc. NATO IST-128 Workshop Cyber Attack Detection, Forensics Attribution Assessment Mission Impact*, 2015, pp. 1–16.

[11] T. Grafenauer, S. König, S. Rass, and S. Schauer, "A simulation tool for cascading effects in interdependent critical infrastructures," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, 2018, pp. 1–8.

[12] D. Lee, D. Kim, M. K. Ahn, W. Jang, and W. Lee, "Cy-through: Toward a cybersecurity simulation for supporting live, virtual, and constructive interoperability," *IEEE Access*, vol. 9, pp. 10041–10053, 2021.

[13] M. R. Stytz and S. B. Banks, "Future challenges for cyber simulation," *J. Defense Model. Simul., Appl., Methodol., Technol.*, vol. 17, no. 1, pp. 47–49, Jan. 2020.

[14] M. Lange, A. Kott, N. Ben-Asher, W. Mees, N. Baykal, C.-M. Vidu, M. Merialdo, M. Malowidzki, and B. Madahar, "Recommendations for model-driven paradigms for integrated approaches to cyber defense," 2017, *arXiv:1703.03306*.

[15] M. Park, H. Lee, Y. Kim, K. Kim, and D. Shin, "Design and implementation of multi-cyber range for cyber training and testing," *Appl. Sci.*, vol. 12, no. 24, 2022, Art. no. 12546.

[16] *ATT&CK*. MITRE. Accessed: May 8, 2023. [Online]. Available: https://attack.mitre.org

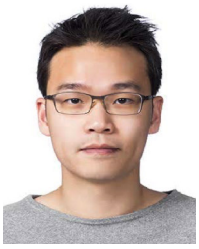
[17] P. Nespoli, D. Papamartzivanos, F. Gómez Mármol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1361–1396, 2nd Quart., 2018.

[18] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, *Special Publication 800-61: Computer Security Incident Handling Guide*, 2nd ed., National Institute of Standards and Technology, Gaithersburg, MD, USA, 2012.
[19] *Guidelines 2010-8, Computer Security Incident Analysis Process Guide*, 3rd ed., Korea Internet & Security Agency (KISA), Naju, South Korea, 2010.
[20] P. Kral, *The Incident Handlers Handbook*, SANS Institute, Rockville Pike, MD, USA, 2011.
[21] M. Maj, R. Reijers, and D. Stikvoort, *Good Practice Guide for Incident Management*, European Network and Information Security Agency (ENISA), Athens, Greece, 2010.
[22] P. Rajivan, M. A. Janssen, and N. J. Cooke, "Agent-based model of a cyber security defense analyst team," in *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 57, no. 1. Los Angeles, CA, USA: SAGE, 2013, pp. 314–318.
[23] E. Hemberg, J. R. Zipkin, R. W. Skowyra, N. Wagner, and U.-M. O'Reilly, "Adversarial co-evolution of attack and defense in a segmented computer network environment," in *Proc. Genetic Evol. Comput. Conf. Companion*, Jul. 2018, pp. 1648–1655.
[24] M. Ge, J. H. Cho, B. Ishfaq, and D. S. Kim, "Modeling and analysis of integrated proactive defense mechanisms for Internet of Things," in *Modeling and Design of Secure Internet of Things*, 2020, pp. 217–247.
[25] D. L. Olson and D. Delen, *Advanced Data Mining Techniques*. Cham, Switzerland: Springer, 2008.
[26] *D3FEND*. MITRE. Accessed: May 8, 2023. [Online]. Available: https://d3fend.mitre.org
[27] (2021). *vsTasker*. VirtualSim. Accessed: May 8, 2023. [Online]. Available: https://www.virtualsim.com/products/vstasker
[28] S. Choi, M. Kim, J. Youn, M. Park, S. Lee, and D. Shin, "A study on cyber resilience evaluation method centered on infringement response time," *J. Defense Secur.*, vol. 4, no. 2, pp. 87–110, 2022.

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.

MYUNG KIL 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.

SEONGKEE LEE received the B.S. degree in mathematics from Dongguk University, South Korea, in 1984, the M.S. degree in computer science from Yonsei University, in 1989, and the Ph.D. degree in computer science from Korea University, in 2003. From 1984 to 1998, he was a Research Fellow with the Korea Institute of Defense Analyses. He was a Visiting Scholar with Syracuse University, USA, in 1994. Since 1999, he has been a Senior Principal Researcher with the Agency for Defense Development. His research interests include software engineering, modeling and simulation, project management, and cyber security. He was certified as a Professional Engineer in the information processing area, in 1991.



DONGHWAN LEE (Member, IEEE) received the B.E. degree in industrial engineering and the M.S. degree in computer science and engineering from Korea University, Seoul, Republic of Korea, in 2006 and 2008, respectively, where he is currently pursuing the Ph.D. degree in cybersecurity. He is a Senior Researcher with the Cyber Technology Center, Agency for Defense Development, Seoul. His research interests include wireless communications, parallel and distributed computing, wireless security, and virtualization technologies for cybersecurity.

MOOSUNG PARK received the B.S. and M.S. degrees in computer science from Sogang University, Seoul, Republic of Korea, in 1988 and 1990, respectively, and the Ph.D. degree in computer engineering from Sejong University, Seoul, in 2023. Since 1990, he has been a Chief Principal Researcher with the Agency for Defense Development, developed Korea C4I system and researched cyber security technology for military systems. His research interests include cyber training systems, AI-based threat analysis, the IoT security, and weapon system security.

DONGKYOO SHIN (Member, IEEE) received the B.S. degree in computer science from Seoul National University, South Korea, in 1986, the M.S. degree in computer science from the 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. From 1986 to 1991, he was with the Korea Institute for 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. He is currently a Professor with the Department of Computer Engineering, Sejong University, South Korea. His research interests include machine learning, ubiquitous computing, bio-signal data processing, and information security.