Article

A Study on Cyber Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement

최세호1, 윤재필1, 김국진1, 4, 이성기2, 권오진3 and 신동규1, 4, \*

|  |
| --- |
| **Citation:** To be added by editorial staff during production.  Academic Editor: Firstname Lastname  Received: date  Revised: date  Accepted: date  Published: date    **Copyright:** © 2022 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/). |

1 Department of Computer Engineering, Sejong University, Seoul 05006, Republic of Korea

2 R.O.K Agency for Defense Development, Seoul 05771, Republic of Korea

3 Department of Electronics Engineering, Sejong University, Seoul 05006, Republic of Korea

4 Department of Convergence Engineering for Intelligent Drones, Sejong University,

Seoul 05006, Republic of Korea

**\*** Correspondence: shindk@sejong.ac.kr

**Abstract:** 알려지지 않은 사이버 위협을 대응하기 위해 다단계 심층 정보보호체계로 방어하고 있지만, 사이버 공격은 정보보호체계의 빈틈을 찾아 역량을 집중시키고 있다. 이러한 상황에서는 제한된 시간 안에 사이버 공격을 100% 대응하지 못한다. 사이버 공격을 인지했을 때 신속한 대응으로 시스템의 정상적인 운영 상태에서 피해가 확산되는 것을 차단해야 한다. 가능한 빠른 시간내에 사이버 공격 전의 상태로 돌아갈 수 있는 지속 가능한 사이버 레질리언스 역량을 갖추어야 한다. 본 논문에서는 사이버 레질리언스의 대응 및 복구단계에 맞게 행동화할 수 있도록 정보시스템의 장애 복구시간을 기초로 사이버 방어활동 최적화 절차를 제안하였다. 훈련 결과와 비교하여 사이버 공격유형별 침해대응시간을 검증하였으며, 전체 대응시간 대비 21%의 단축되는 개선효과가 있었다. 지속적인 사이버 레질리언스 평가 활동으로 대응시간을 최적화한다면 사이버 공격으로 발생된 피해에 대한 복구시간을 예측하는데 활용이 가능할 것이다. 향후에는 사이버 방어활동별 대응시간을 세분화하여 사이버 전투력 지수에 대해 연구를 수행할 예정이다.

**Keywords:** 사이버 레질리언스; 침해대응시간; 사이버 방어활동; 복구시간 목표

1. 서론

우리는 손쉽게 접할 수 있는 스마트폰과 IoT(Internet of Things) 장비 등 다양한 매체를 활용하여 인터넷이라는 사이버 공간에 항시 접속해 있다. 지금의 사이버 공간은 우주에 국경이 없는 것처럼 전 세계인들과 함께 공존하는 인프라로 구축되어 있다. 문제는 급변하는 인프라 환경에 맞게 완벽한 정보보호체계가 부재하여 언제든지 사이버 공간에서 악의적인 활동이 진행되고 있다. 또한 조직화 및 특정 정부의 지원을 받으면서 피해 규모와 심각성이 지속적으로 증가되고 있다. 그 가운데 알려지지 않은 지능형 사이버 위협은 공공 및 민간 등 모든 조직에서 대응하는데 현실적으로 문제점 및 한계에 직면하고 있다 [1]. 민간 기업에서는 2013년부터 정보보호관리체계(Information Security Management System)를 통해 적합한 정보보호 정책을 수립하고 보완하면서 시시각각 발생되는 사이버 공격에 상시 대응하는 등 여러 보안대책을 유기적으로 통합 관리하기 위해 노력하고 있다. 그러나, 피해상황을 실시간으로 인지하고 분석 및 대응하는 역량은 부족한 실태이다 [2].

이러한 상황에서는 제한된 시간 안에 사이버 공격을 100% 대응하지 못한다. 사이버 공격을 인식했을 때 신속한 대응으로 시스템 운영 상태에서 피해가 확산되는 것을 차단해야 한다. 또한, 가능한 빠른 시간내에 사이버 공격 전의 상태로 돌아갈 수 있는 지속 가능한 사이버 레질리언스 역량을 갖추어야 한다.

본 논문은 사이버 레질리언스의 대응 및 복구단계에 맞게 행동화할 수 있도록 구성했다. 2장에서 사이버 레질리언스와 사이버공격 대응시간, 복구시간에 대한 연구 동향을 요약한다. 3장에서는 사이버 방어활동 최적화 절차와 대응시간 측정 방안을 제안한다. 4장에서는 사이버 공격에 대한 실제 대응훈련 결과와 비교하여 사이버 공격유형별 대응시간을 검증하고 5장은 결론과 향후 연구방향에 대해 제시하고자 한다.

2. 관련연구

2.1. 사이버 레질리언스

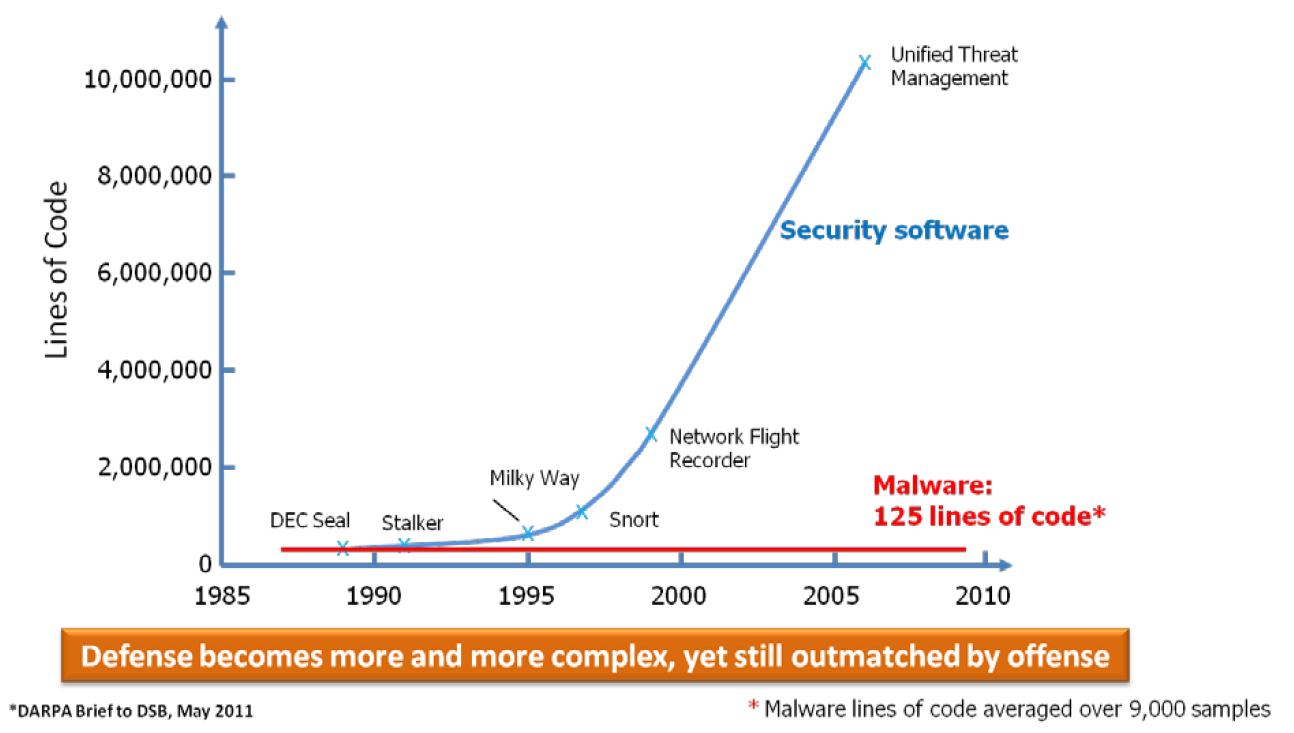
사이버 레질리언스(Cyber Resilience)는 조직이 사이버보안 침해를 당하더라도 목표한 성과를 지속적으로 거둘 수 있는 역량을 의미한다. 2012년 다보스에서 개최된 세계경제포럼(World Economic Forum)에서는 사이버 레질리언스를 시스템 및 조직이 평균 중단시간과 평균 복구시간의 조합으로 측정한 사이버 이벤트를 견딜 수 있는 능력으로 정의하였다 [3]. 이러한 사이버 레질리언스 프레임워크는 식별, 보호, 탐지, 대응, 복구의 5가지 단계로 구성된다 [4].

사이버 공격은 ‘언젠가는’이 아닌 ‘언제나’ 일어날 수 있는 현실이다. 일반적으로 소프트웨어를 최신 버전으로 유지하는 것이 정보보호의 최선책이라고 생각한다. 그러나, 2022년 Ponemon 보고서에서 소프트웨어 취약점으로 발생된 사이버 공격은 18% 밖에 되지 않았다. 무엇보다 심각한 것은 사이버 공격은 다양한 매체에서 발생되고 있으며, 공격자가 조직에 침투하는데 사용하는 공격요소들이 나날이 발전하여 일상화되고 있다는 점이다.

클라우드, IoT 인프라 환경, 블록체인, 그리고 글로벌화 되는 공급망 운영 같이 복잡성과 불확실성이 그 어느 때보다 사이버 공격으로 큰 피해를 당할 수 있는 환경입니다. 이에 효과적으로 대응하기 위해 사이버 레질리언스 대응 전략을 도입하고 사전 예방적이고 통합된 접근 방식을 취해야 한다. 대부분의 침해 사실을 내부에서 인식하지 못하고 유관기관으로부터 통보받거나 또는 공격자에 의해 공개되는 경우가 많다. 이러한 사이버 공격을 인식한 후 어떠한 방법으로 대응하느냐가 중요하다 [3]. 사이버 공격에 신속하게 대응하고 가능한 빨리 사이버 공격 전의 상태로 돌아가는 것이다. 이렇게 사이버 레질리언스는 사이버 공간에서의 방어활동으로 예상되거나 예상치 못한 모든 위협의 부정적인 영향을 흡수하여 원상태로 복구할 수 있는 조직의 역량이다.

사이버 위협은 새로운 것이 아니지만 그 위협은 하루가 다르게 예측 불가능하게 확대되고 있다. 사이버 공격이 발생하기 전에 탐지하고 예방하는 것도 어렵고, 특정 사이버 공격에 대해 알려진 하나의 일치하는 방어기술로 대응하는 것도 쉽지 않다 [6]. 사이버 공격은 더 이상 단일 이벤트가 아니라 지속적이고 끈질긴 이벤트가 될 가능성이 높다. 만병통치약도 없고 모든 인프라에 맞는 단일 솔루션도 없으며, 대부분의 경우 사이버 공격으로부터 보호할 수 있는 단일 접근 방식도 없다 [6]. 기업은 지속적으로 보안 조치를 취하는 대신 가장 중요한 자산을 식별하고 현재 사이버 방어활동과 어떻게 관련되어 있는지 분석해야 한다. 사이버 레질리언스를 적용하여 의사결정권자에게 방안을 추천하고 신속대응 및 임무수행 보장을 지원하는 패러다임 전환이 필요하다.

DARPA는 방어용 소프트웨어와 공격용 소프트웨어 크기 사이의 증가하는 격차를 **Figure** 1과 같이 제시했다. 네트워크를 방어하는 소프트웨어의 복잡성은 보호하려는 시스템의 복잡성 증가로 인해 시간이 지남에 따라 기하급수적으로 계속 증가하고 있지만, 평균적으로 성공적인 공격에 사용되는 소프트웨어 코드의 크기는 거의 일정하게 유지된다 [7]. 방어는 가능한 모든 공격으로부터 보호해야 하지만, 공격은 방어의 가장 약한 지점에 대해 모든 자원을 집중시키면 된다.



**Figure 1. 방어용 소프트웨어와 공격용 소프트웨어의 크기 비교 [7]**

Huang et al. 은 RL(Reinforcement Learning) 기반 CRM(Cyber-Resilient Mechanism)을 제안했다. RL-CRM은 APT(Advanced Persistent Threat)공격에 전략적으로 대응한다. 그리고 공격을 당했을 때는 중요기능과 성능을 유지함으로써 본래 기능을 보존한다 [8].

Babiceanu et al. 은 가상 제조 네트워크 설계 단계의 요구 사항 캡처에 사용할 SDN 기반 제조 테스트베드와 결합된 사이버 보안-레질리언스 온톨로지를 제안했다. 그 중 IIoT 시스템 네트워크는 사용 가능한 복원력 메커니즘을 사용하여 중단 이벤트에 반응한다 [9].

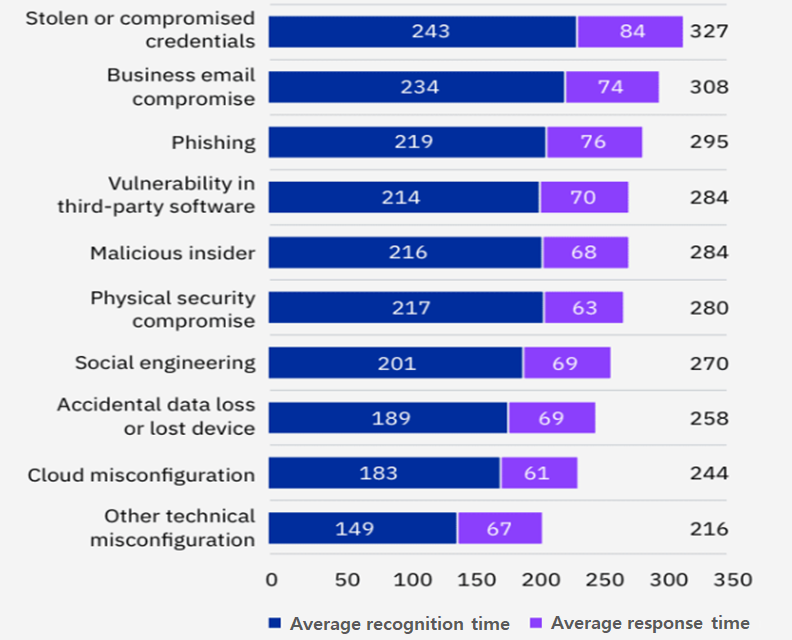
Haque et al. 은 산업 제어 시스템에 대한 사이버 복원력 척도를 계산하기 위해 확장된 형태의 R4 레질리언스 프레임워크를 활용한다. 이를 통해 프레임워크와 주관적 설문 방법을 사용하여 정성적 사이버 레질리언스 평가 도구를 제안했다. 평가 도구는 탄력성 계산 절차에 대한 자세한 수학적 설명을 제공한다 [10].

Ligo et al. 은 효과적인 사이버 레질리언스 대책 개발에 대한 연구 및 실천 방향을 제안했다. 사이버 레질리언스의 새로운 측정법을 개발하려면 기능을 정의하는 적절한 방법이 필요하다. 그리고, 복구자의 노력에 의해 복구되는 사이버 레질리언스의 척도를 정의해야 한다고 주장했다 [11].

사이버 레질리언스에 대한 관련 연구들을 조사했다. 그 결과 각 연구들에서 주장하는 사이버 레질리언스의 개념이 조금씩 다른 것을 확인할 수 있었다. 그에 따라 본 연구에서는 사이버 레질리언스는 위에서 정의한 바와 같이 사이버 공격을 당할 수 있다는 것을 인정하고 사이버 방어활동으로 예상되거나 예상치 못한 모든 위협의 부정적인 영향을 흡수하여 최단시간내에 공격 전의 원상태로 복구할 수 있는 조직의 역량으로 정의한다. 그리고 정보보호체계 평균 대응시간과 정보시스템 장애 최소 복구시간을 기초로 사이버 레질리언스를 평가한다.

2.2. 사이버공격 대응시간

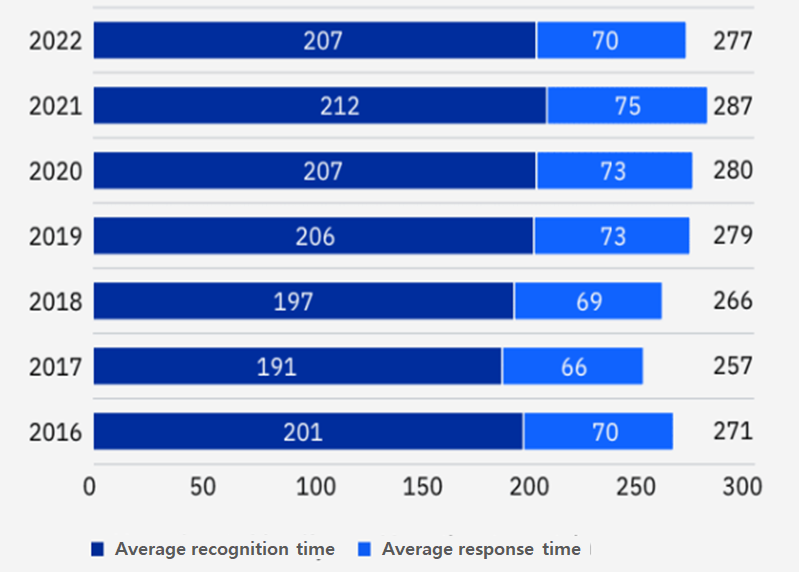
Ponemon은 IBM의 후원을 받아 데이터 유출 비용을 분석하는 연구소이다. 2021년 3월부터 2022년 3월까지 17개 국가 및 지역에서 의료, 에너지, 재무 등 17가지 산업분야에 걸쳐 실제로 사이버 공격이 발생하여 비정상적인 경로로 데이터가 유출된 사례를 **Figure** 2와 같이 분석하였다.

**** **Figure 2. 공격유형별 인식 및 대응까지의 소요되는 시간 [12]**

조사에 의하면 사이버 공격을 인식하는데 평균 207일이 소요되고 데이터 유출을 인식하고 대응하는 시간도 평균 70일이 소요되어 전체 라이프사이클은 277일이었다. 1월 1일에 데이터 유출을 위해 최초 사이버 공격이 발생할 경우 이를 인식하고 대응하기까지 277일이 소요되므로 10월 4일까지 사이버 공 격에 대한 완벽한 대응은 없었다 [12].

도난 또는 손상된 인증정보를 이용한 사이버 공격의 경우 인식까지 243일, 대응까지 84일이 소요되어 평균적으로 327일이라는 가장 오랜 시간이 소요되었다. 이 시간은 사이버 공격을 인식하고 대응하는데 평균시간보다 18%가 많이 소요되었다. 비즈니스 이메일을 이용한 사이버 공격은 인식 및 대응까지 라이프사이클이 308일로 두번째로 길었다. 그리고, 타사 소프트웨어 취약점을 이용한 사이버 공격 또한 인식 및 대응에 284일이 소요되어 네 번째로 라이프사이클이 길었다.

다른 조사로, 2016년부터 2022년까지 **Figure** 3과 같이 연도별 사이버 공격을 인지하고 대응하는 평균시간을 비교 분석하였다 [12]. 평균시간이 2017년도에 일시적으로 감소하였다가 점차적으로 2021년도에 증가된 것처럼 사이버 공격 인식 및 대응기술이 발전함에 따라 사이버 공격요소 및 침투기술도 나날이 발전하고 있다는 것을 알 수 있다. 그러므로 사이버 공격에 대응하기 위해 새로운 역량이 필요하다.



**Figure 3. 연도별 사이버 공격을 인지하고 대응하는 평균시간 [12]**

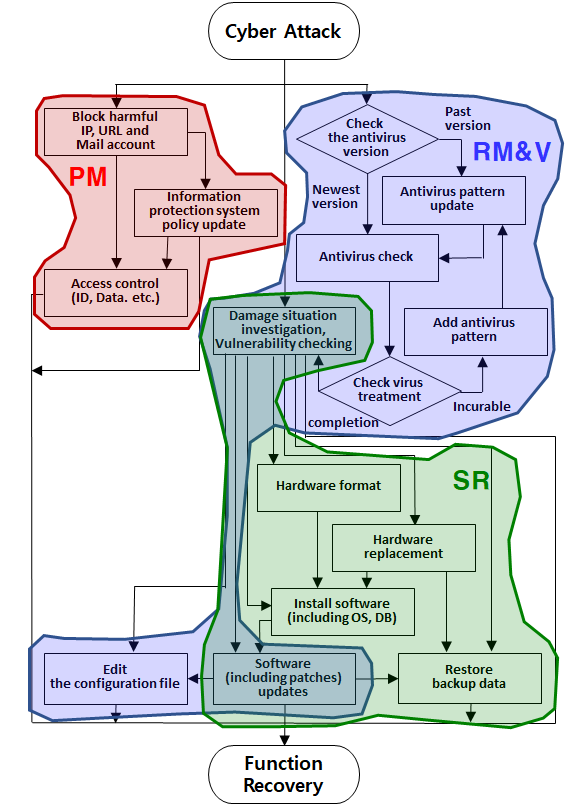
2.3. 복구시간

복구시간은 전투피해평가의 기능적 피해평가 요소 중 하나로, 표적화된 공격대상이 보유한 기능을 복구하거나 대체하는데 소요되는 시간을 의미하며, 보유한 기능을 복구되는데 가장 빠른 가능시간(최소)과 가장 빠른 현실적 시간(최대)으로 설정한다. 그리고, 표적처리 목표 및 가용첩보에 기반하여 전투피해평가 수행시 부분적으로 복구시간 판단을 포함할 수 있다. 표적화된 공격대상의 모든 기능 복구에 최대 10일의 소요시간을 판단할 수 있지만, 고유기능의 50% 복구는 최소 2일이 소모될 수도 있다. 경우에 따라 고유기능의 50%만 복구되어도 수행능력 유지가 가능할 수 있다 [13].

3. 사이버 방어활동 최적화와 대응시간 측정

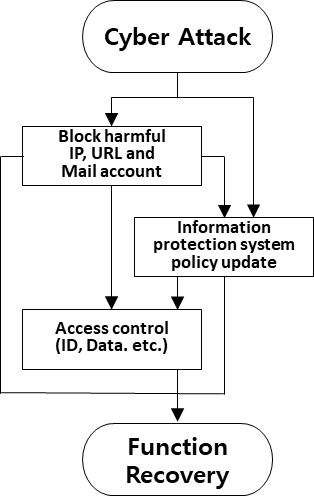
3.1. 사이버 공격에 대한 사이버 방어활동 최적화

사이버 공격에 대해 사이버 레질리언스의 대응 및 복구단계에 맞게 행동할 수 있도록 **Figure** 4와 같이 사이버 방어활동 최적화 절차를 제안한다. 악의적인 사이버 공격이 성공했을 경우 조기에 피해 확산을 차단하기 위해 정보보호체계 정책 업데이트 등 정책관리(Policy Management, 이하 PM)를 최신화하면서, 동시에 2차 추가 공격에 대비하여 악성코드 및 취약점을 제거(Remove Malware and Vulnerability, 이하 RM&V)해야 한다. 그 후 피해를 받은 기능을 정상화시키기 위해 시스템복원(System Restore, 이하 SR) 등 적극적으로 대응해야 한다 [14].



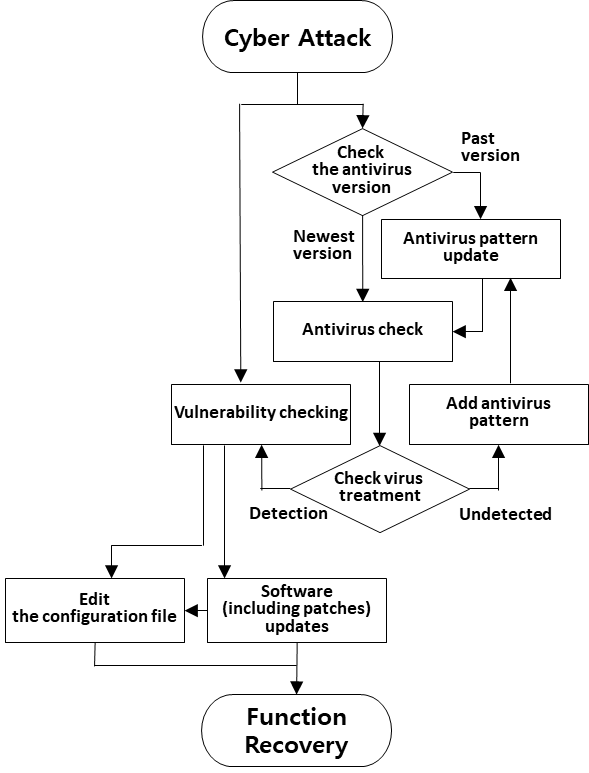
**Figure 4. 사이버 공격에 대한 사이버 방어활동 최적화 절차**

정책관리(PM) 분야는 **Figure** 5와 같이 정보보호체계의 보안정책을 관리하여 피해확산 및 동일한 사이버 공격을 차단한다. 피해확산을 줄이기 위해 방화벽(Firewall), 해킹메일차단을 활용하여 내·외부로 이동되는 유해 IP/URL, 메일계정을 차단한다. 침입방지체계(Intrusion Prevention System, 이하 IPS), 웹방화벽(Web Firewall), 바이러스 방역체계의 탐지정책을 최신정보로 업데이트하여 알려진 사이버 공격에 대한 네트워크 패킷 분석 및 웹페이지 위·변조 행위를 시그니처 기반으로 차단하거나 악성코드를 탐지하여 해당 파일을 격리시킨다. 통합접근관리(Extranet Access Management), 보안운영체제(SecureOS) 등을 활용하여 계정에 따라 권한을 차등 부여하거나 데이터의 접근을 통제할 수 있다.



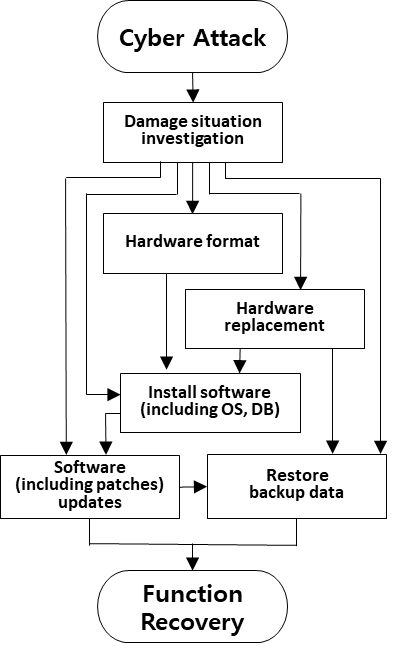
**Figure 5. 사이버 방어활동 정책관리(PM) 분야**

악성코드 및 취약점 제거(RM&V) 분야는 **Figure** 6과 같이 바이러스 방역체계로 악성코드와 악성코드가 설치된 취약한 경로를 찾아 제거하여 사이버 공격 전 상태로 회복한다. 악성코드와 취약점 제거하는 담당자가 각각 있어서, 동일한 시간대에 점검하여 조치한다면 침해대응시간은 단축될 수 있을 것이다. 여기서는 정책관리(PM) 분야에서 유해 IP/URL을 차단했다는 전제하에 악성코드를 제거한 후 취약점을 제거한다. 악성코드를 제거하기 위해 바이러스 방역체계 패턴을 최신화 시킨 후 점검하고, 탐지가 안 될 경우에는 악성코드 샘플을 확보하여 신규 패턴을 추가 후 바이러스를 치료한다. 악성코드 제거 후에는 취약점 점검도구를 활용하여 취약점을 확인한다. 그런 다음 웹 개발 프로그램 및 데이터베이스의 취약한 버전을 최신 또는 권장하는 상위 버전 이상으로 설치하기 위해 현재 동작중인 응용소프트웨어간의 영향성을 반드시 확인하여 취약점을 보완한다. 만약 응용소프트웨어의 영향성이 있을 경우에는 소스파일이 수정될 때까지 서비스를 차단하거나 악의적으로 사용되지 않도록 사용자의 접근을 최소화한다. 또한, 사이버 공격에 악용되는 서비스가 기본 파일에 존재할 경우 환경설정 파일을 수정한다.



**Figure 6. 사이버 방어활동 악성코드 및 취약점 제거(RM&V) 분야**

시스템복원(SR) 분야는 **Figure** 7과 같이 서버, 스토리지, 정보보호체계, 네트워크 등 사이버 자산의 피해 상황을 조사하여 하드웨어와 소프트웨어를 사이버 공격 전 상태로 회복한다. 단순 소프트웨어 오류는 최신 버전으로 설치하고 동일 사례가 재발할 경우 관련 소프트웨어를 재설치(삭제 후 재부팅 필요) 후 최신 버전으로 업데이트한다. 하드웨어가 문제일 경우에는 포맷 후 관련 소프트웨어를 재설치하고 백업 파일을 복원한다. 다만, Appliance(별도의 OS나 SW 설치없이 전원을 ON하면 바로 사용할 수 있는 장비) 제품일 경우에는 하드웨어 교체 후 백업 파일을 복원한다.



**Figure 7. 사이버 방어활동 시스템복원(SR) 분야**

이렇게 정책관리(PM)는 공격대상의 IP주소 정보를 기반으로 방화벽(Firewall), 침입방지체계(IPS) 등 정보보호체계를 활용하여 수평적(동일한 시간에 여러 가지 업무를 같이 수행)으로 보안정책을 최신화할 수 있다. 그리고, 악성코드 및 취약점 제거(RM&V)와 시스템복원(SR)은 물리적인 공격대상에 SW(OS, DB 등)설치 및 실행 등 수직적(순차적으로 업무 수행)으로 대응활동이 진행된다. 일반적인 시간 흐름으로 정책관리(PM)와 악성코드 및 취약점 제거(RM&V)는 동일한 시간대에 각각 사이버 방어활동을 진행할 수 있으나, 시스템복원(SR)은 2차 사이버 공격을 차단하기 위해 악성코드 및 취약점 제거(RM&V)가 완료된 후 사이버 방어활동을 수행해야 한다. 그러나, HW 포맷 및 교체될 경우에는 3가지 사이버 방어활동 분야가 혼합으로 진행될 수도 있다.

3.2. 정보시스템 자원별 목표복구시간

정보시스템 자원별 장애처리 절차는 정보시스템을 구성하는 주요 자원에 대해 발생할 수 있는 시스템 장애를 사전에 문서화한다. 그리고 시스템 운영조직 간의 의사소통을 원활히 하고, 주요 장애의 예상 장애원인 및 복구시간 등을 추정하는데 참고될 수 있도록 해야 한다 [15]. 그리고 정보시스템 담당자는 자원별 장애처리 절차를 주기적으로 검토하고 훈련함으로써 실제 운영환경에서 발생하는 정보시스템 장애에 대해 적절히 대응할 수 있는 능력을 갖추어야 한다.

자원별 장애처리 절차는 실제 운영환경에 적용하면서 개선사항이 있으면 수시로 보완되어 관련 담당자에게 배포되고 숙지되어야 한다. 또한, 장애 파악을 위한 점검순서는 해당 장애현상에 대해 장애원인을 제공할 가능성이 높은 부분에 대해 우선적으로 점검하도록 작성된다.

한국지능정보사회진흥원(과거 한국전산원)에서는 장애처리의 복구시간목표 (Recovery Time Objective, 이하 RTO)를 **Table** 1과 같이 제시하였다. 각 기관에서는 자원별 장애처리시 운영하는 시스템 자원의 특성에 따라 적절한 절차와 복구시간을 지정해야 한다.

**Table 1. 정보시스템별 장애조치 소요시간 [15]**

|  |  |  |
| --- | --- | --- |
| **Type** | **Cause of disability** | **Time(Minute)** |
| Web Server | One bad web server disk | 60 |
| Two or more bad web server disks | 120 |
| Excessive share of resources (CPU, Memory, Disk) per process | 5 |
| Operating system corruption | 5 |
| Bad LAN card | 30 |
| Application  Software | Application software error | 60 |
| Data error | 60 |
| Batch job error | 60 |
| Database  and  Middleware | Oracle process stopped/abnormal | 10 |
| Oracle archive files full | 10 |
| Oracle listener stopped/abnormal | 10 |
| Oracle home directory full | 10 |
| Oracle block corruption | 60 |
| MQ process stopped/abnormal | 10 |
| MQ config file change abnormal | 10 |

정보시스템 자원별 장애처리 절차는 주요 자원에 대해 장애원인을 파악한 후 그 장애를 조치하기 위한 작업절차를 기술하였다. 정보시스템의 자원은 서버, 응용소프트웨어, 네트워크, 데이터베이스 등을 말한다. 여기에는 장애를 근본적으로 해결하기 위한 절차 및 그러한 여유가 없는 경우에 사용할 수 있는 응급조치 방법이 모두 포함되어 있다. 장애조치 목표시간은 장애원인을 파악하여 장애조치가 모두 완료되어 정상 동작시까지의 시간을 의미한다.

3.3. 공공기관의 장애별 복구 소요시간

공공기관에서는 소관 영역의 정보시스템에 장애관리 정책을 정의하여 표준화된 장애처리를 가능하게 함으로써 운영의 효율성을 높이기 위해 노력하고 있다. 이를 위해 정보시스템 장애의 유형과 장애 해결 유형에 대한 기준을 수립하여 장애이력을 관리하고 있으며, 분기별 정보시스템 운영결과 보고서를 통해 장애관리현황을 분석하고 있다 [16].

본 저자가 운영하는 공공기관의 2021년 장애관리현황을 통해 복구일시를 **Table** 2와 같이 정리하였다. 이는 한국지능정보사회진흥원과 달리 장애원인을 파악하는데 소요되는 시간이 포함되어 있어 동일 장애에 대해서는 최소시간을 반영하였다.

**Table 2. 공공기관 정보시스템별 장애조치 소요시간 [16]**

|  |  |  |
| --- | --- | --- |
| **Type** | **Cause of disability** | **Time(Minute)** |
| Web Server | Defective voltage regulator module | 101 |
| Excessive share of resources (CPU, Memory, Disk) per process | 85 |
| Bad memory card | 81 |
| LAN card setting error | 117 |
| Application  Software | Application software error | 185 |
| Batch job error | 75 |
| Excessive antivirus memory usage | 32 |
| Hang occurs | 68 |
| Database  and  Middleware | DB forced restart | 96 |
| Oracle archive files full | 153 |
| Oracle listener log capacity full | 90 |

3.4. 사이버 방어활동별 대응시간 도출

사이버 공격으로 발생된 피해를 원상태로 복구하는 것은 정보시스템 장애 발생 후 시스템 복원절차와 동일하므로 사이버 방어활동별 대응시간을 다음과 같이 판단하였다.

사이버 방어 대상은 정보보호체계, 시스템, 네트워크, PC 등 사이버 자산으로 한다. 침해대응시간은 사이버 공격이 발생한 후 원하는 작업 성능에 도달하기 위해 걸리는 시간을 복구시간 목표(Recovery Time Objective, 이하 RTO)로 설정한다. 공공기관의 2021년 ‘장애처리현황’ 조치사항별 복구일시와 한국지능정보사회진흥원의 ‘정보시스템 자원별 장애처리 절차’ 장애원인별 복구시간 목표를 바탕으로 사이버 공격에 대해 방어활동별 대응시간을 **Table** 3과 같이 도출하였다. 일부 방어활동은 실제 데이터 수집 및 바이러스 방역체계 제작업체의 기본 설정 값을 적용하였다.

**Table 3. 사이버 방어활동간 대응시간 [15, 16]**

|  |  |  |
| --- | --- | --- |
| **Type** | **Response Activity** | **Time(Minute)** |
| Policy  Management | Block harmful IPs, URLs, and Mail accounts | 10 |
| Information protection system policy update | 20 |
| Access control (ID, Data. etc.) | 10 |
| Remove  Malware and  Vulnerability | Antivirus check | 40 |
| Antivirus pattern update | 60 |
| Add antivirus pattern | 360 |
| Damage situation investigation,  Vulnerability checking | 30 |
| Edit the configuration file | 10 |
| Software (including patches) updates | 60 |
| System  Restore | Hardware format | 30 |
| Hardware replacement | 60 |
| Install software (including OS, DB) | 1,440 |
| Restore backup data | 60 |

4. 사이버 공격유형별 사이버 레질리언스 평가

국방부의 ‘국방 사이버 위기대응 실무매뉴얼’에 따라 사이버 공격 발생시 침해탐지, 초동조치, 분석, 복구 순으로 대응활동이 진행된다 [17]. 일반적으로 사이버 공격은 은닉기술이 적용되어 여러 국가를 경유하여 공격하거나 공격자의 실체도 가상일 수 있다. 원인 규명, 추가 피해여부 확인, 대응수준 판단, 공격주체 식별 등 조사·분석]이 개인 및 조직의 역량에 따라 결과의 질이 달라질 수 있다 [18]. 그러므로 매뉴얼대로 전용프로그램을 실행하거나 정해진 양식에 수집된 정보를 입력하면 대응활동을 추천해 주는 시스템이 필요하다. 2022년 후반기 훈련 결과를 본 논문의 **Figure** 4에서 제시한 사이버 방어활동 최적화 절차와 비교하여 행동화가 가능한 범위내에서 정책관리(PM), 악성코드 및 취약점 제거(RM&V), 시스템복원(SR)의 사이버 레질리언스 대응 및 복구단계 중심으로 침해대응시간을 검증하고자 한다.

4.1. DDoS 공격에 대한 방어활동 및 대응시간

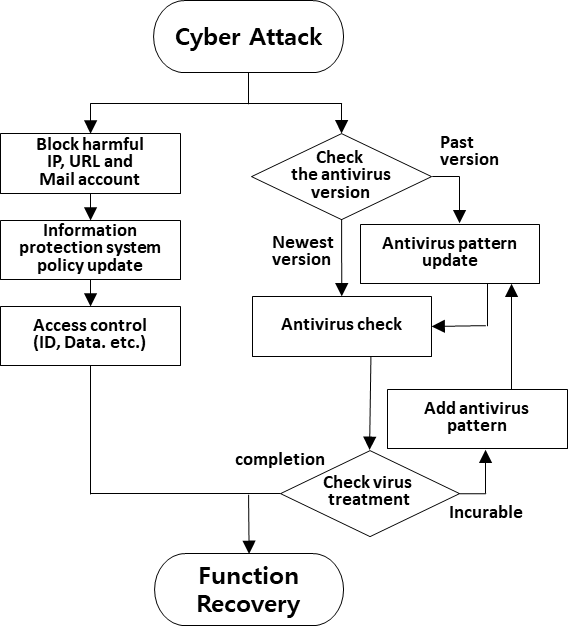
2022년 0월 0일 06시 00분, 국내·외 IP와 공공기관 내부 IP에서 A홈페이지를 대상으로 DDoS 공격이 탐지되었으며, 지속적인 공격으로 홈페이지 접속 지연이 발생하였다. 정보보호체계를 이용한 유해 패킷 차단과 좀비 PC에 대한 대응이 필요한 상황이다.

사이버 방어활동은 **Table** 4와 같이 정책관리(PM) 측면에서는 홈페이지로 접근하는 비정상적인 IP를 차단하기 위해 Timeout 설정 값을 낮추거나 중복되는 특정 패킷 시그니처를 찾는다. 악성코드 및 취약점 제거(RM&V) 측면에서는 악성코드에 감염된 PC를 치료하기 위해 유관기관과 공조하거나 공공기관 내부 감염된 PC의 악성코드 샘플을 확보하여 바이러스 패턴을 최신화한다.

**Table 4. DDoS 공격에 대한 사이버 방어활동 및 대응시간 [15, 16]**

|  |  |  |
| --- | --- | --- |
| **Type** | **Response Activity** | **Time(Minute)** |
| Policy  Management | Block harmful IPs, URLs, and Mail accounts | 10 |
| Information protection system policy update | 20 |
| Access control (ID, Data. etc.) | 10 |
| Remove  Malware and  Vulnerability | Antivirus check | 40 |
| Antivirus pattern update | 60 |
| Add antivirus pattern | 360 |

실제 훈련에서는 A홈페이지 서버에서 사용자와의 Timeout 설정 값을 조절하여 일정 시간동안 Session을 유지시켰다. 침입방지체계(IPS)에서 Get 요청의 개행 문자(\r\n)가 한 번만 표시되는 패킷을 시그니처로 차단 [19]하여 06시 45분에 서비스가 정상화 되었다. 후속조치로 악성코드에 감염된 공공기관 내부 좀비 PC를 치료하기 위해 바이러스 패턴을 추가 요청하여 17시 15분(11시간 15분 경과)에 훈련과 관련된 유해트래픽이 발생되지 않았다. DDoS 공격에 대한 방어활동은 **Figure** 8과 같이 연결된다.



**Figure 8. DDoS 공격에 대한 방어활동 연결도**

DDoS 공격에 대해 사이버 방어활동 최적화 절차와 대응시간을 비교하면 정책관리(PM)로 40분, 악성코드 제거(Antivirus check + Add antivirus pattern + Antivirus pattern + Antivirus check)로 500분이 소요된다. 정책관리(PM)와 악성코드 제거는 동시에 행동화 할 수 있는 수평적 대응활동으로 악성코드 제거 대응시간과 동일한 총 8시간 20분이 소요되어 실제 훈련 대응시간(11시간 15분) 대비 2시간 55분이 감소하였다.

4.2. 홈페이지 변조에 대한 방어활동 및 대응시간

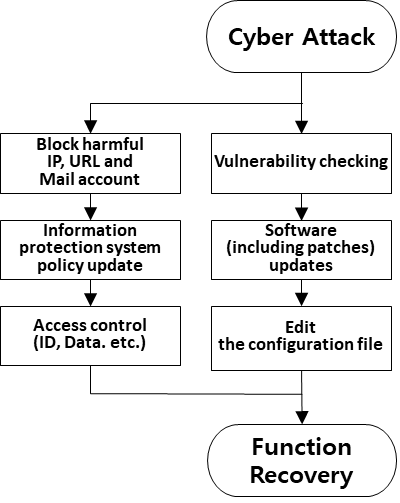
2022년 0월 0일 10시 00분, 중국 IP에서 공공기관 내부 IP로 불법 접근이 탐지되었으며, B홈페이지의 팝업창 변조가 발생하였다. 홈페이지 소스파일에서 보안 설정이 미설정되어 취약점을 이용한 공격으로 소스파일 접근권한 변경 및 오픈소스 게시판에 대한 보안 패치가 필요한 상황이다.

사이버 방어활동은 **Table** 5 와 같이 정책관리(PM) 측면에서는 외부 IP로부터의 관리자 페이지 접근을 모두 통제하고 접근권한을 점검한다. 악성코드 및 취약점 제거(RM&V) 측면에서는 웹페이지 프로그램을 최신 버전으로 업데이트한다.

**Table 5. 홈페이지 변조에 대한 사이버 방어활동 및 대응시간 [15, 16]**

|  |  |  |
| --- | --- | --- |
| **Type** | **Response Activity** | **Time(Minute)** |
| Policy  Management | Block harmful IPs, URLs, and Mail accounts | 10 |
| Information protection system policy update | 20 |
| Access control (ID, Data. etc.) | 10 |
| Remove  Malware and  Vulnerability | Vulnerability checking | 30 |
| Edit the configuration file | 10 |
| Software (including patches) updates | 60 |

실제 훈련에서는 게시판을 최신 버전으로 보안패치하고, 업로드 파일 확장자와 외부에서 관리자 웹페이지로 접근하는 권한을 통제하여 11시 35분(1시간 35분 경과)에 홈페이지 팝업창이 정상화 되었다. 홈페이지 변조에 대한 방어활동을 **Figure** 9와 같이 연결된다.



**Figure 9. 홈페이지 변조에 대한 방어활동 연결도**

홈페이지 변조에 대해 사이버 방어활동 최적화 절차와 대응시간을 비교하면 정책관리(PM)로 40분, 취약점 제거로 100분이 소요된다. 정책관리(PM)와 취약점 제거는 동시에 행동화 할 수 있는 수평적 대응활동으로 취약점 제거 대응시간과 동일한 총 1시간 40분이 소요되어 실제 훈련 대응시간(1시간 35분) 대비 5분이 증가하였다.

4.3. 정보보호체계 중단에 대한 방어활동 및 대응시간

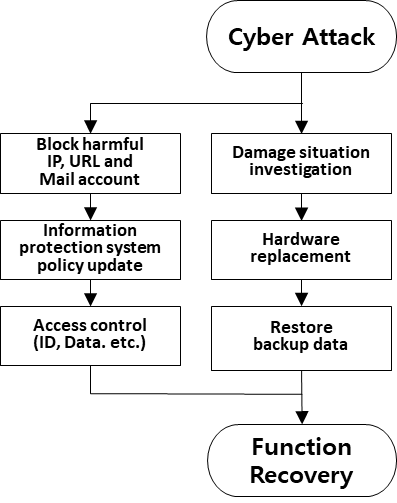
2022년 0월 0일 14시 00분, 미국 IP에서 공공기관 내부 IP로 불법 접근이 탐지되었으며, WAN영역에 운용중인 방화벽에 Down 메시지가 발행하였다. 이중화 구성되어 있어 외부 서비스 지원에는 영향이 없으나 해당 방화벽은 접속이 불가한 상태이다. 강제로 재부팅을 시도하였으나 정상기동이 불가하고, CF메모리(OS 및 정책 정보를 저장하는 비휘발성 메모리) 불량으로 긴급 장비 교체가 필요한 상황이다.

사이버 방어활동은 **Table** 6 과 같이 정책관리(PM) 측면에서는 정보보호체계로 직접 접근하려는 외부 IP를 차단한다. 시스템복원(SR) 측면에서는 정보보호체계의 피해 상황을 조사하여 대체장비를 확보하고, 백업된 데이터를 복원한다.

**Table 6. 정보보호체계 중단에 대한 사이버 방어활동 및 대응시간 [15, 16]**

|  |  |  |
| --- | --- | --- |
| **Type** | **Response Activity** | **Time(Minute)** |
| Policy  Management | Block harmful IPs, URLs, and Mail accounts | 10 |
| Information protection system policy update | 20 |
| Access control (ID, Data. etc.) | 10 |
| System  Restore | Damage situation investigation | 30 |
| Hardware replacement | 60 |
| Restore backup data | 60 |

실제 훈련에서는 대체장비 확보 및 교체, 백업된 정책 및 환경설정 파일을 복원하여 17시 05분(3시간 5분 경과)에 기능이 정상화되었다. 정보보호체계 중단에 대한 방어활동을 **Figure** 10 과 같이 연결된다.

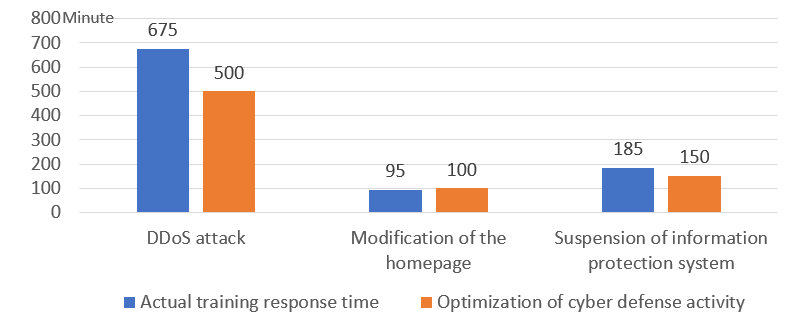


**Figure 10. 정보보호체계 중단에 대한 방어활동 연결도**

정보보호체계 중단에 대해 사이버 방어활동 최적화 절차와 대응시간을 비교하면 정책관리(PM)로 40분, 시스템복원(SR)으로 150분이 소요된다. 정책관리(PM)와 시스템복원(SR)은 동시에 행동화 할 수 있는 수평적 대응활동으로 시스템복원(SR) 대응시간과 동일한 총 2시간 30분이 소요되어 실제 훈련 대응시간(3시간 5분) 대비 35분이 감소하였다.

4.4. 사이버 레질지언스 대응시간 분석

2022년 후반기 훈련 내용 중 3가지 공격유형을 사이버 방어활동 최적화 절차와 비교하였다. 사이버 레질리언스 대응시간을 분석한 결과 **Figure** 11 과 같이 정책관리(PM)는 타 대응분야와 분산처리로 사이버 침해대응시간에 영향이 낮았다. 그러나, 악성코드 및 취약점 제거(RM&V)과 시스템복원(SR)은 순차적으로 처리되어 사이버 침해대응시간에 주로 영향을 주는 것으로 확인되었다.



**Figure 11. 사이버 레질리언스 대응시간 비교 결과**

사이버 방어활동은 모든 이해관계자가 익숙한 경우에만 원활하게 동작된다 [20]. 이렇게 훈련이나 실제로 행동화된 대응활동으로 검증된 대응시간을 지속적으로 분석한다면 **Table** 3보다 사이버 방어활동은 더욱 세분화될 것이다. 또한, 대응시간은 최신 상태로 유지 [21]되어 정확성과 신뢰성은 높아질 것이다.

5. 결론

우리는 알려지지 않은 사이버 위협을 대응하기 위해 다단계 심층 정보보호체계로 방어 [22]하고 있지만, 사이버 공격은 정보보호체계의 빈틈을 찾아 역량을 집중시키고 있다. 이러한 상황을 대응하기 위해 사이버 레질리언스 역량을 지속적으로 평가하고 최적의 방책으로 숙달하여 가능한 빠른 시간내에 사이버 공격 전의 상태로 돌릴 수 있는 방법론과 대응 절차가 필요하다.

본 논문에서는 사이버 공격을 인식하여 대응 및 복구하기까지의 대응시간을 기준으로 사이버 레질리언스 대응 및 복구단계에 맞게 사이버 방어활동 최적화 절차를 제안하고 검증하였다. 그 결과 전체 대응시간 대비 21%의 단축시켜 사이버 공격에 대한 신속한 복구능력을 제고할 수 있었다. 그리고 지속적인 사이버 레질리언스 평가 활동으로 대응시간을 최적화 [23]하여 사이버 공격발생시 피해복구시간을 예측하는데 활용되길 기대한다.

향후에는 사이버 전장관리체계 연구에 기여할 수 있도록 사이버 방어활동에 대한 영향도와 긴급도를 반영하고, 소관영역 대상으로 정보보호체계, 시스템, 네트워크 등 사이버 자산의 운용상태를 평가하여 사이버 공격 발생시 실시간으로 피해현황을 가시화할 수 있는 사이버 전투력 지수에 대해 연구를 수행할 예정이다.

**Author Contributions:** For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used “Conceptualization, X.X. and Y.Y.; methodology, X.X.; software, X.X.; validation, X.X., Y.Y. and Z.Z.; formal analysis, X.X.; investigation, X.X.; resources, X.X.; data curation, X.X.; writing—original draft preparation, X.X.; writing—review and editing, X.X.; visualization, X.X.; supervision, X.X.; project administration, X.X.; funding acquisition, Y.Y. All authors have read and agreed to the published version of the manuscript.” Please turn to the [CRediT taxonomy](https://img.mdpi.org/data/contributor-role-instruction.pdf) for the term explanation. Authorship must be limited to those who have contributed substantially to the work reported.

**Funding:** This work was supported by a National Research Foundation of Korea (NRF) grant

funded by the Korea government (MSIT) (No. 2022R1F1A1074773).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

**Abbreviations**

The following abbreviations are used in this manuscript:

IoT Internet of Things

ISMS Information Security Management System

RL Reinforcement Learning

CRM Cyber-Resilient Mechanism

APT Advanced Persistent Threat

SDN Software Defined Networking

IIoT Industrial Internet of Things

R4 Robustness, Redundancy, Resourcefulness, and Rapidity

PM Policy Management

RM&V Remove Malware and Vulnerability

SR System Restore

IPS Intrusion Prevention System

RTO Recovery Time Objective

DDoS Distributed Denial of Service

References

1. Choi, S.H.; Oh, H.R.; Yun, J.B. A Study on Command and Control Through Cyber Protection Function Analysis, Journal of the Korea Institute of Military Science and Technology, Daejeon, Republic of Korea, October 2021; Vol 24, No. 5, pp. 537-544.
2. Kim, K.H. Overview of Information Security Management System Certification System and Development Direction, Korea Internet & Security Agency, Seoul, Republic of Korea, October 2017; pp. 3-7.
3. Ryu, J.G. Respond to cyber security incidents that you don't know when not if, IDG Summary IBM, USA, October 2018.
4. Frank, D.; Phil, G. Five Key Technologies for Enabling a Cyber Resilience Framework, IDC White Paper, USA, October 2020.
5. Lee, S.K.; Lee, S.H.; Kang, T.I.; Kwon, M.Y.; Lee, N.B. Resiliency of Mobile OS Security for Secure Personal Ubiquitous Computing, Personal and Ubiquitous Computing, 2018.
6. WHITE PAPER, The Cyber Resilience Blueprint: A New Perspective on Security, Symantec, USA, September 2014.
7. Defense Science Board, Resilient Military Systems and the Advanced Cyber Threat, Department of Defense, USA, January　2013.
8. Huang, Y.; L. Huang; Q. Zhu. Reinforcement learning for feedback-enabled cyber resilience. Annual Reviews in Control, 2022; pp. 273-295.
9. Babiceanu, R.F.; R. Seker. Cyber resilience protection for industrial internet of things: A software-defined networking approach. Computers in industry, 2019. 104; pp. 47-58.
10. Haque, M.A.; S. Shetty; B. Krishnappa. ICS-CRAT: a cyber resilience assessment tool for industrial control systems. in 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). 2019; pp. 273-281.
11. Ligo, A.K.; A. Kott; and I. Linkov. How to measure cyber-resilience of a system with autonomous agents: Approaches and challenges. IEEE Engineering Management Review, 2021. 49(2); pp. 89-97.
12. Ponemon Institute, Cost of a Data Breach Full Report 2022, IBM Security, USA, July 2022; pp. 14-18.
13. Chairman of The Joint Chiefs of Staff Instruction 3162.02, METHODOLOGY FOR COMBAT ASSESSMENT, U.S. Joint Chiefs of Staff, USA, March 2019; pp. C-7.
14. Cyber Operations Department, Guidelines for Performing Cyber Operations, R.O.K Joint Chiefs of Staff, Republic of Korea, February 2021; pp. 25-37.
15. National Computerization Agency, Guideline for Incident & Problem Management Information System, Office of Government Policy Coordination · Ministry of Information and Communication, Seoul, Republic of Korea, December 2005; pp. 20-31, 94-96.
16. 2021 1/4 - 4/4 Information System Operation Result Report, Public Institution, Republic of Korea, 2021.
17. Cyber Response Force Team, Defense Cyber Crisis Response Practical Manual, R.O.K Ministry of National Defense, Seoul, Republic of Korea, November 2021.
18. Joint Education President 17-1, Joint Cyber Operations, R.O.K Joint Chiefs of Staff, Republic of Korea, December 2017; pp. 6-11.
19. Internet Infringement Response Center, DDoS Attack Response Guide, Korea Internet & Security Agency, Seoul, Republic of Korea, August 2021; pp. 60.
20. Marsh, Cyber resilience: Twelve key controls to strengthen your security, Marsh, New York, USA, April 2022; pp. 19-20.
21. Cyber Security & Operational Systems Resilience, New Zealand's Financial Markets Authority, New Zealand, June 2022; pp. 6.
22. Choi, S.H.; Oh, H.R.; Yun, J.B. A Study on Defense Indicators for Evaluation of Defense Cyber Response System, 2019 Korea Institute of Military Science and Technology an Academic Conference for Estimating, Daejeon, Republic of Korea, November 2019; pp. 646-647.
23. The Cyber Resilience Index: Advancing Organizational Cyber Resilience, 2022 World Economic Forum, Geneva, Switzerland, July 2022; pp. 14.

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.