Journal of the KIMST, Vol. 24, No. 5, pp. 537-544, 2021
ISSN 1598-9127(Print) · 2636-0640(Online)
DOI https://doi.org/10.9766/KIMST.2021.24.5.537

Technical Paper 정보·통신 부문

사이버 방호기능 분석을 통한 지휘통제에 관한 연구

최세호[1] · **오행록**[2] · **윤주범**[*,1]

[1] 세종대학교 정보보호학과
[2] 국방과학연구소 제2기술연구본부

A Study on Command and Control Through Cyber Protection Function Analysis

Seho Choi[1] · Haengrok Oh[2] · Joobeom Yun[*,1]

[1] *Department of Computer and Information Security, Sejong University, Korea*
[2] *The 2nd Research and Development Institute, Agency for Defense Development, Korea*

(Received 16 April 2021 / Revised 19 July 2021 / Accepted 20 August 2021)

Abstract

Cyber threats can bypass existing cyber-protection systems and are rapidly developing by exploiting new technologies such as artificial intelligence. In order to respond to such cyber threats, it is important to improve the ability to detect unknown cyber threats by correlating heterogeneous cyber protection systems. In this paper, to enhance cyber-attack response capabilities, we proposed command and control that enables rapid decision-making and response before the attack objectives are achieved, using Lockheed Martin's cyber kill chain and MITRE ATT&CK to analyze the purpose and intention of the attacker.

Key Words : Cyber Threat(사이버 위협), Cyber Protection Function(사이버 방호기능), Command and Control(지휘통제)

1. 서 론

지금 우리 사회는 모든 것이 사물인터넷(IoT)으로 연결되어 시간과 장소에 구애받지 않고 원하는 정보를 클라우드(Cloud)에 보관하였다가 언제든지 불러올 수 있다. 또한 인공지능(AI)을 이용하여 빅데이터 기술을 누구나 손쉽게 일상생활에서 활용하고 있다. 산업현장도 실제공간과 사이버공간의 정보가 직·간접적으로 공유되고 있는 제4차 산업혁명 시대에 살고 있으며, 공공·민간기관, 국방 등 특정 영역에 구분없이 국가 전반에서 디지털화가 확산되었다. 모든 주체의 활동 기반이 사이버공간으로 확대됨에 따라 사이버 공격이 지능화·표적화·고도화·조직화를 통해 개인, 기업을 넘어 한 나라의 국가 안보까지 영향을 줄 만큼 사이버 위협이 심각하게 증가하고 있다[1]. 최근 사이버 공격은 현재 운용중인 사이버 방호체계를 우회할 수 있는 능력을 보유한 가운데 인공지능(AI) 등

* Corresponding author, E-mail: jbyun@sejong.ac.kr

신기술을 악용하여 지능화되고 있다. 금전 및 정보 탈취 목적의 표적화된 랜섬웨어와 사회적, 시기적 이슈를 활용한 고도화된 피싱 및 스미싱 같은 신종 사이버 위협이 조직화되어 대응의 어려움은 날로 증가하고 알려지지 않은 사이버 위협에도 노출되어 있다[2]. 이에 정부에서는 2019년 4월, '국가 사이버안보 전략'을 수립했으며, 사이버 공격에 대한 대응역량을 고도화하기 위해 사이버전 대비 전략·전술을 개발하고 사이버 전력체계 보강 업무를 추진하고 있다. 사이버 전력체계의 보강을 위해서는 사이버 방호기능을 분석하여 선제적으로 사이버 위협을 예측할 수 있는 대응역량이 필요하다.

따라서, 본 논문에서는 사이버 전력체계를 강화하기 위한 방안으로 록히드마틴이 2011년에 발표한 사이버 킬 체인(Cyber Kill Chain)[3]과 MITRE ATT&CK(Adversarial Tactics, Techniques and Common Knowledge) 등의 검증된 모델을 적용하여 현재 운용중인 사이버 방호체계의 한계점을 도출하고, 사이버 공격단계별 대응책을 검토하고자 한다. 또한 공격자의 목적과 의도를 파악하기 위해 사이버 방호체계에서 수집된 정보와 최신 사이버 위협 동향을 분석하고, 사이버 공격이 목적을 달성하기 이전에 신속히 대응할 수 있도록 사이버 상황관리·자산 통합평가·위협경보 분석 등과 같은 의사결정을 지원하는 지휘통제를 제안하고자 한다.

본 논문의 2장에서는 록히드마틴의 사이버 킬 체인 및 MITRE ATT&CK 모델과 사이버 킬 체인 개선 방안에 대한 연구 동향을 요약한다. 3장에서는 MITRE ATT&CK 모델과 공격기술(전술, 기법 및 절차 : Tactics, Techniques and Procedures, 이하 TTPs)을 사이버 킬 체인 공격단계로 분석하여 설명한다. 4장에서는 사이버 공격에 대응하기 위한 방호기능을 분석하고 공격 단계별로 대응하기 위한 방호기능을 맵핑한다. 5장에서는 개별적으로 운용중인 사이버 방호기능을 통합하여 의사결정을 지원하는데 효과적인 지휘통제 방안을 제안하고 6장은 결론과 향후 연구방향에 대해 제시하는 순으로 논문을 구성한다.

2. 사이버 킬 체인 관련 연구 동향

본 장에서는 서론에서 간략히 설명한 록히드마틴의 사이버 킬 체인 공격절차와 방어유형, MITRE의 ATT&CK 모델을 소개하고 공격 원점지 타격을 위한 사이버 킬 체인 전략과 사이버 위협 분석 및 개선 방안에 대한 연구 내용을 요약한다.

2.1 록히드마틴의 사이버 킬 체인[4]

사이버 킬 체인(Cyber Kill Chain)은 군사적 개념의 킬 체인(Kill Chain)을 적용한다. 사이버 공격도 일련의 과정을 거치며, 방어자가 공격 과정에서 한 단계만 차단해도 공격자가 다음 공격 단계로 진행이 제한되는 것에 착안하여 공격절차와 방어유형을 제시했다.

공격절차는 정찰, 무기화, 전달/유포, 악용, 설치, 명령/제어, 목적 달성의 7단계로 Table 1과 같이 구성된다.

Table 1. Attack procedure of cyber kill chain

공격절차	주요 내용
정찰	공격목표와 대상을 조사, 식별, 선정
무기화	자동화 도구 등을 이용하여 공격을 위한 사이버 무기 준비
전달/유포	공격대상에게 사이버 무기 전달
악용	취약점을 이용하여 사이버 무기 작동
설치	공격대상에게 악성 프로그램 설치
명령/제어	공격대상을 원격 제어하기 위한 채널 구축
목적 달성	정보수집, 파괴 등 소기의 목적 달성

방어유형은 미국 합참 정보작전 교리 대응 방안을 적용하여 방어자가 사이버 공격에 맞춤식으로 대처할 수 있는 탐지, 거부, 교란, 약화, 기만, 파괴의 6가지로 구분하고 Table 2와 같이 유형별로 활용할 수 있는 기술을 제시했다[5].

Table 2. Cyber kill chain defense types

방어유형	주요 내용
탐지	공격자의 정보 수집 행위를 발견
거부	공격자의 접속이나 사용을 거절
교란	공격자를 혼란에 빠뜨려 방해
약화	공격행위의 효율이나 효과를 감소
기만	거짓 정보를 통해 잘못된 판단을 유도
파괴	공격 도구가 계획된 기능을 수행하지 못하도록 통제하고 복원이 불가능하게 조치

2.2 MITRE의 ATT&CK 모델[6]

MITRE는 미국 연방정부의 지원을 받는 비영리 연구개발단체로 사이버 킬 체인을 이용하여 공격자의 각 행위들을 공격기술(TTPs)로 분류한 ATT&CK 모델[7]을 제안했다. 실제로 일어났던 사이버 공격 사례를 분석하여 최신 공격전술과 침투기술, 대응절차 등 사이버 위협 모델 및 방법론을 개발하기 위한 프레임워크를 제공해 주고 있다.

MITRE ATT&CK 모델과 공격기술(TTPs)은 지속적으로 업데이트 되고 있으며, 요약하면 Table 3과 같다[8].

Table 3. MITRE ATT&CK update summary[8]

날짜		주요 내용
2017	1월	해킹그룹 프로필 추가
	7월	MacOS/Linux용 기술 추가
2018	4월	PRE-ATT&CK 및 Mobile용 기술 추가
2019	4월	ATT&CK의 완화(Mitigations)기술 추가
	10월	Cloud용 기술 추가
2020	10월	PRE-ATT&CK가 새로운 전술로 대체

요약한 내용을 포함해 2015년부터 2020년 10월까지 엔터프라이즈(Windows, MacOS, Linux, Cloud) 및 모바일(Android, iOS) 기술, 해킹그룹 및 소프트웨어가 13차례에 걸쳐 전체 또는 부분적으로 최신화되고 있다.

2.3 공격 원점지 타격을 위한 사이버 킬 체인 전략[9]

군사적 개념의 킬 체인(Kill Chain)과 동일한 절차인 감시정찰(Sensor) - 결심(Decision) - 타격(Strike)의 3단계에 연동체계(System of Systems)가 추가된 사이버 킬 체인 전략을 다음과 같이 제시하였다.

첫째, 감시체계는 통제 가능한 내부 네트워크 뿐만 아니라 통제가 제한되는 외부 네트워크에서 탐지되는 이상(anomaly) 현상도 수집한다. 둘째, 결심체계는 각종 감시자산으로부터 수집되는 다양한 정보를 빅데이터 기술로 분석하여 공격의 정당성을 확보한다. 셋째, 타격체계는 물리적 전쟁으로 확대를 방지하기 위해 위험이 낮은 공격원점 타격과 좀비PC 같은 지원세력까지 공격하는 확대 타격 그리고 위협행위를 설계한 지휘세력까지 포함한 타격으로 구분한다. 마지막으로 넷째는 감시 - 결심 - 타격 체계가 유기적으로 작동하기 위해 연동체계가 구축되어야 한다고 제시했다.

2.4 사이버 위협 분석 및 개선 방안[10]

사이버 킬 체인에서 지능형 사이버 위협에 대한 기존의 사이버 방호체계의 한계점을 도출하고 효과적으로 개선된 대응방안을 다음과 같이 제시하였다.

지능형 사이버 위협은 공격대상의 잠재된 사회공학적 취약점을 공략하기 때문에 운용중인 사이버 방호체계로는 대응에 한계가 있으므로 방어가 100 % 완벽할 수 없다는 점을 인정해야 한다. 이를 개선하고 대응할 수 있는 사이버 방호체계 대책을 수립하고 구축해야 한다고 강조했다. 사이버 공격은 계획된 시나리오에 따라 진행되며 모든 공격단계가 실행될 경우 최종 목적이 달성되므로 사이버 방어의 패러다임도 알려진 패턴 기반 탐지와 차단에서 공격 체인 분석과 연결 고리 차단으로 개선한다. 사이버 킬 체인 기반으로 사이버 방호체계의 대응능력을 향상시키기 위해서는 공격 준비단계인 무기화단계, 방어 측면에서 사이버 공격을 초기단계에 진압하는데 주요한 역할을 하는 약화단계, 공격을 무력화시킬 수 있는 기만단계에 대응하기 위한 사이버 킬 체인 지능형 방호체계 개선 방안을 제시했다.

3. 사이버 킬 체인을 활용한 공격기술 분석

공격단계는 록히드마틴의 사이버 킬 체인을 적용하고 공격단계에 적용된 기술은 MITRE에서 제안한 공격기술(TTPs)을 활용한다.

MITRE의 12개 공격영역에 속한 공격기술(TTPs)의 특성을 기준으로 공격단계와 연계하여 재분류한 과정은 Fig. 1과 같으며, 2개 이상의 공격단계에 중복되어 적용된 공격기술(TTPs)도 있다.

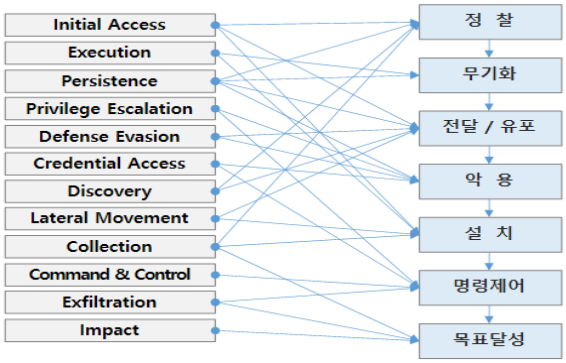

Fig. 1. MITRE attack technology reclassified to cyber kill chain stage

MITRE가 전세계 해커 그룹의 공격기술(TTPs)을 분석하고 유형화한 공격기술(TTPs)과 사이버 킬 체인의 공격단계, 공격대상을 분류하면 Fig. 2와 같이 구성된다.

MITRE 공격기술		사이버 킬 체인 공격단계							공격대상				
TTPs 코드	공격 TTPs명	정찰	무기화	전달/유포	악용	설치	명령제어	목적달성	네트워크	서버	단말기	응용체계	보호관리
T1001	데이터 난독화						O		O				
T1002	데이터 압축							O		O	O		
T1003	인증정보 획득				O	O				O	O		
T1004	Winlogon Helper DLL					O				O	O		
T1005	로컬시스템 데이터 수집					O				O	O		
T1006	파일 시스템 논리 오프셋				O					O	O		
T1007	시스템 서비스 발견					O				O	O		
T1008	대체 채널						O		O				
T1009	바이너리 패딩		O		O					O	O		
T1010	응용 프로그램 창 발견					O					O		
T1011	다른 네트워크 매체를 통한 데이터 유출						O	O	O				
T1012	쿼리 레지스트리					O				O	O		
T1013	포트 모니터					O				O	O		
T1014	루트킷(RootKit)		O			O				O	O		
T1015	접근성 기능				O	O				O	O		
T1016	시스템 네트워크 구성 발견					O				O	O		
T1017	응용 프로그램 배포 소프트웨어			O						O	O		
T1018	원격 시스템 발견	O				O				O	O		
T1019	시스템 펌웨어					O				O	O		
T1020	자동화된 유출							O		O	O		
T1021	원격 서비스			O				O		O		O	
T1022	데이터 암호화							O	O				
T1023	바로가기 수정					O					O		
T1024	맞춤형 암호화 프로토콜						O		O				
T1025	이동식 미디어 내 데이터					O				O	O		
T1026	멀티밴드 통신						O		O				
T1027	난독화된 파일 또는 정보				O	O				O	O		
T1029	예약 전송							O		O	O		
T1030	데이터 전송 크기 제한							O	O				

Fig. 2. Examples of attack technology classification

사이버 킬 체인 공격단계로 분류된 공격기술(TTPs)로부터 방어해야 할 공격대상은 네트워크, 서버, 단말기(PC), 응용체계, 보호관리 등의 5가지로 구분하였다.

MITRE의 공격기술(TTPs)에 대응하기 위한 방호기능을 반드시 공격대상이 대응할 필요는 없다. 즉, 서버에 대한 공격기술(TTPs)이 반드시 서버에서만 대응하는 것을 의미하는 것은 아니며, 서버에 대한 공격을 사전에 네트워크에서 대응하거나 응용체계 및 보호관리 관점에서 대응할 수 있다는 의미이다.

4. 사이버 방호기능 분석

사이버 공격에 대응하기 위한 방호기능은 MITRE의 탐지, 거부, 교란, 약화, 기만, 파괴의 6가지 방어유형과 각 기능을 통합할 수 있는 지휘통제를 추가하여 Table 4와 같이 분류한다.

사이버 방호기능은 2019년에 국내 473개 업체가 정보보안 시스템으로 개발하고, 상용화된 사이버 방호체계가 가지고 있는 공통된 핵심기능을 기준으로 도출한다. 정보보호산업의 특성상 제품과 서비스의 통합 및 융합은 매우 빠르게 진행되고 있어 분류 기준을 과거의 하드웨어, 소프트웨어, 서비스의 3가지 분야로 구분하는 것은 모호해졌다. 그래서 한국정보보호산업협회(KISIA)에서는 정보보호산업 관련 학계 및 산업계의 전문가들로부터 상용화된 제품에 대한 심층적인 조사를 통해 정보보호산업을 재분류했다. 그 중에서 정보보안 시스템의 구성을 방어위치 기준으로 네트워크보안, 시스템보안(PC 포함), 정보유출방지, 암호/인증, 보안관리 5가지로 분류하고 Table 5와 같이 방호기능을 식별한다[11].

Table 4. Protection function according to defense type

방어유형	내용	방호기능
탐지	공격행위에 대한 발견	공격자 또는 비정상 행위의 정보를 발견하는 단계로써 다른 방어유형(거부, 교란, 약화, 기만, 파괴)과 연계됨 예) 악성코드 탐지, 트래픽 분석
거부	접근 및 사용 통제	공격자 또는 비정상 행위의 접근 및 사용하는 행위 차단함 예) OS보안패치, 화이트리스팅
교란	방어를 통한 흐름 방해	공격자의 행위 또는 공격을 위한 정보 흐름을 방해하는 단계로써 다른 방어유형(거부, 기만)과 연계됨 예) IPS로 비정상 행위 차단
약화	공격자의 결정과 행동 범위 축소	공격행위의 효율 감소 및 행동 범위를 축소하여 공격대상의 가치를 저하 시킴 예) Anti-DDoS로 유해트래픽 차단
기만	거짓정보 유포 또는 정보 조작	공격대상 및 수집한 정보의 사실을 조작하여 공격자에게 잘못된 판단을 하도록 유도함 예) 허니팟, 허니넷
파괴	태세전환	악성코드가 계획된 기능을 수행하지 못하도록 시스템 및 정보를 통제하고 복원이 불가능하도록 조치함 예) 바이러스방역체계로 파일 삭제
지휘통제	사이버 작전을 통한 임무달성	진행 상황을 실시간으로 제공하여 가시화하고 공유함으로써 상황판단과 지휘결심을 효율적으로 지원함 예) SIEM 기반으로 대응절차 지능화

Table 5. Identification of protection functions by protection target

방어위치	방호기능	사이버 방호체계
네트워크	대량으로 유입되는 트래픽을 분석하여 네트워크의 연속성 보장함	DDoS차단시스템
	트래픽 분석 및 프로토콜 필터링이 가능하며 IP/PORT를 차단함	방화벽, UTM
	IPS 및 애플리케이션을 인식하고, 제어기능을 포함하여 위협을 동적으로 차단함	차세대방화벽
	네트워크 패킷을 분석하여 시그니처 기반으로 트래픽을 차단함	IPS
	웹페이지 위변조 및 유해트래픽을 실시간 감시하여 차단함	웹방화벽
	미등록 PC와 Agent 미설치 PC의 네트워크를 탐지하여 차단함	NAC
	무선통신장치를 모니터링하고 미등록된 AP 통신을 차단함	무선네트워크보안
	인가된 사용자에 대해 전용회선과 동등한 서비스로 안전하게 원격접속을 허용함	VPN(가상사설망)
	내·외부로 망을 구분하고 격리함으로써 외부 위협으로부터 내부망을 보호함	망분리(가상화)
시스템(PC 포함)	시스템상으로의 모든 접근과 작업을 통제하고 작업 모니터링 및 로그기록을 저장함	시스템접근통제
	정보 유출과 악성코드 식별하고 불법적으로 접근 권한을 취득한 소프트웨어를 식별하여 차단함	멀웨어대응, 램섬웨어대응
	특정 E-mail 주소, 서버 IP, 제목과 내용, 다수인원에게 전송 여부 등을 검사하여 차단함	스팸차단솔루션
	시스템 접근 및 권한 남용을 제한하고 권한 내 정보 접근을 허용함	보안운영체제(SecureOS)
	시그니처 기반 악성코드 탐지 및 악성코드 우회/회피를 차단하고 임의로 변경된 파일을 삭제함	바이러스방역체계, APT대응
	모바일 내 오피스, 뱅킹, 전자 화폐 등 서비스상에서 발행할 수 있는 위협으로부터 보호함	모바일보안
	패턴화된 이미 알려진 악성코드와 달리 바이러스방역체계에서 탐지 못하는 신종 행위분석기반 악성코드를 식별하여 차단함	엔드포인트탐지및대응
정보유출방지	인가되지 않은 변경, 파괴, 노출 및 비일관성 행위로부터 보호함	DB보안
	비인가 사용자가 볼 수 없도록 데이터를 은폐함	DB암호
	사용자 식별 및 복제방지가 가능하고 분실시 데이터를 보호함	보안USB
	데이터 외부 전송 모니터링과 위변조를 방지하고 진위 확인 및 문서 암호화가 가능함	DRM
	데이터 외부전송 및 정보유출 탐지와 발송메일을 모니터링함	DLP
암호/인증	일회용 동적 비밀번호를 생성 및 인증함으로써 분실을 예방함	개인인증(OTP포함)
	데이터의 비밀성, 무결성, 인증, 부인방지 및 접근을 제어함	공개키기반구조(PKI)
	사용자에 따라 사용 권한을 차등 부여하는 접근을 관리함	통합접근관리(EAM)
	시스템별 접속시 아이디와 비밀번호를 각각 입력하지 않고 한번의 인증으로 전체 시스템을 하나의 시스템처럼 사용함	싱글사인온(SSO)
	사용자 아이디와 비밀번호를 종합적으로 관리해 주는 역할 기반의 사용자 계정 관리	통합계정관리(IM/IAM)
보안관리	정밀 분석된 네트워크 트래픽 및 공격형태를 상관 분석하고 체계적으로 위협을 모니터링함	TMS (위협관리시스템)
	각종 사이버 방호체계 및 시스템에서 발생되는 정보를 통합 연동하여 공격 패턴 분석과 악성코드 수집함	SIEM (통합보안관제시스템)
	취약점을 보완하기 위해 배포되는 패치 파일을 원격에서 자동 설치하고 목록화함	PMS(패치관리시스템)
	자료 손실을 예방하기 위해 지정된 곳에 보관관리 후 복구함	백업 및 복구 관리시스템
	악성코드 민감도와 열린 포트 등 알려진 취약점을 분석함	취약점분석체계

사이버 킬 체인의 공격절차 및 방어유형을 기준으로 공격기술(TTPs)에 대응하기 위한 방호기능을 상용화된 사이버 방호체계에서 식별하였다. Table 6과 같이 사이버 킬 체인에 기반한 사이버 방호체계를 맵핑한다.

Table 6. Cyber kill chain based cyber protection functional product analysis

구분	탐지	거부	교란	약화	기만	파괴
정찰	DDoS차단시스템, 방화벽, IPS, UTM, 차세대방화벽, 웹방화벽, VPN, TMS, SIEM, APT대응, 엔드포인트탐지및대응, 랜섬웨어대응, 멀웨어대응, 보안USB, 바이러스방역체계, 시스템접근통제, 통합접근관리, 무선네트워크보안, 모바일보안	방화벽, UTM, 차세대방화벽, 시스템접근통제, 통합접근관리, 랜섬웨어대응, 멀웨어대응, 보안USB, 모바일보안	방화벽, UTM, 차세대방화벽, 웹방화벽, APT대응, 엔드포인트탐지및대응, 랜섬웨어대응, 멀웨어대응, 보안USB, 바이러스방역체계, 무선네트워크보안	VPN, 랜섬웨어대응, 멀웨어대응, 보안USB, 개인인증솔루션, 공개키기반구조, 통합접근관리/싱글사인온, 통합계정관리	-	바이러스방역체계
무기화	-	-	-	-	-	-
전달/유포	방화벽, IPS, UTM, 차세대방화벽, 웹방화벽, 스팸차단솔루션, TMS, APT대응, 망분리	방화벽, 차세대방화벽, NAC	방화벽, UTM, 차세대방화벽, 스팸차단솔루션, 바이러스방역체계, APT대응, 엔드포인트탐지및대응	NAC	-	바이러스방역체계
악용	방화벽, IPS, UTM, 차세대방화벽, 웹방화벽, TMS, APT대응, 엔드포인트탐지및대응, 바이러스방역체계, 망분리	랜섬웨어대응, 멀웨어대응, 모바일보안, 보안USB	방화벽, UTM, 차세대방화벽, 랜섬웨어대응, 멀웨어대응, 보안USB, PMS	랜섬웨어대응, 멀웨어대응, PMS, 보안USB, 취약점분석체계, 모바일보안	-	바이러스방역체계, PMS
설치	방화벽, IPS, UTM, 차세대방화벽, TMS, APT대응, 랜섬웨어대응, 멀웨어대응, 보안USB, 바이러스방역체계	방화벽, UTM, 차세대방화벽, 랜섬웨어대응, 멀웨어대응, 보안USB, 모바일보안	방화벽, IPS, UTM, 차세대방화벽, 스팸차단솔루션, 멀웨어대응, 모바일보안, 보안USB, 보안운영체제	멀웨어대응, 모바일보안, 보안USB, 보안운영체제	-	-
명령/제어	SIEM, 스팸차단솔루션, DLP, 보안운영체제	DLP, 보안운영체제	DDoS차단시스템, 스팸차단솔루션, APT대응, 보안운영체제	보안운영체제	-	-
목적달성	DDoS차단시스템, 방화벽, IPS, UTM, 차세대방화벽, SIEM, DB보안	DLP, DRM, DB보안	방화벽, UTM, 차세대방화벽, DLP	DDoS차단시스템, DLP, DRM, DB보안, DB암호	-	-

5. 사이버 방호기능을 통합한 지휘통제 제안

알려지지 않은 사이버 위협 중 사이버 방호체계에서 우연하게 탐지된 하나의 위협 정보를 기준으로 피해를 분석하고 대응책을 판단하는 것은 제한된 정보로 인해 잘못된 상황 판단을 할 수 있다.

이러한 잘못된 판단을 보완하기 위해 신규로 탐지된 위협에 대해 소관 네크워크 환경에서 운용중인 사이버 방호체계, 시스템, 네트워크장비 등 사이버 자산에서 관련된 정보를 최대한 수집하여 위협 영향도를 분석하고 대응책의 우선순위를 자동으로 추천해 주거나 의사결정을 통해 지휘결심 할 수 있도록 지원하기 위해 다음과 같은 지휘통제가 필요하다.

5.1 사이버 상황관리체계

예방, 관제, 조사분석, 대응 등 현재 진행중이거나 완료된 모든 사이버 상황에 대해 업무별 진행 상황을 실시간으로 인식하고 상황평가, 의사결정, 업무통제 등 통합적으로 시각화할 수 있는 사이버 상황관리체계를 Fig. 3과 같이 구축한다[12]. 사이버 상황 및 위협 상황을 효과적으로 인식하고 신속·정확한 상황판단을 통한 최적의 의사결정으로 직면한 사이버 위협에 대해 맞춤식 대응역량을 강화한다.

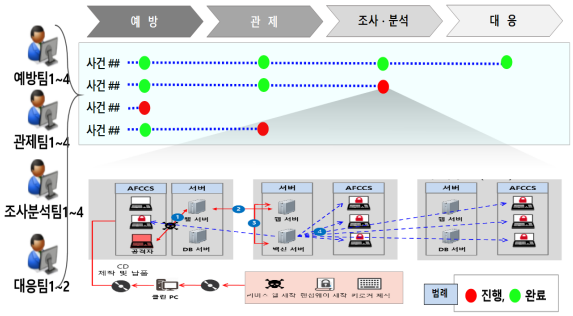

Fig. 3. Configuration of cyber situation management system[12]

5.2 사이버 자산 통합평가체계

네트워크상에서 운용중인 모든 사이버 자산에 대해 자동으로 인식하고 동적으로 변동되는 자산 정보를 주기적으로 최신화하여 시각화할 수 있는 사이버 자산 통합평가체계를 Fig. 4와 같이 구축한다[12]. 사이버 방호체계, 시스템, 네트워크장비 등 모든 자산의 기본 제원과 업데이트 정보, 식별된 취약점 정보까지 데이터베이스로 구축하여 실시간 가시화를 통해 사이버 자산에 대한 상태평가 및 취약점 관리역량을 강화한다.

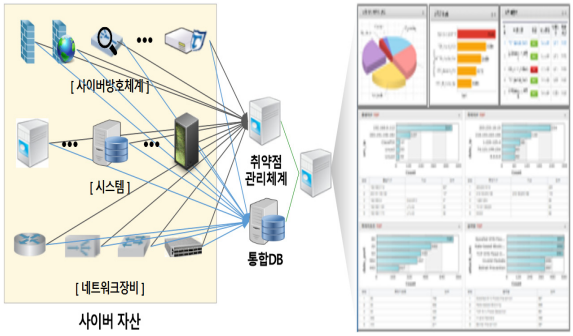

Fig. 4. Configuration of the integrated cyber asset evaluation system[12]

5.3 사이버 위협경보 분석체계

방화벽, IPS, 웹방화벽, APT대응, 바이러스방역체계 같은 사이버 방호체계와 라우터, 백본 등 네트워크장비에서 탐지된 모든 위협 정보는 SIEM으로 종합한다. 이러한 사이버 위협경보에 대한 상관관계를 지능형모델을 통해 공격 경로를 자동으로 제공하고, 공격기술(TTPs)에 대한 대응책을 평가 및 우선순위를 추천 할 수 있는 사이버 위협경보 분석체계를 Fig. 5와 같이 구축한다[12]. 심층분석된 위협 정보를 바탕으로 공격 경로를 구성하고, 수집된 사이버 위협간 연관관계를 분석하여 발생 가능한 사이버 위협상황를 시각화하여 제공한다. 이러한 사이버 위협상황에 대한 최적의 대응책을 추천하고 대응결과 분석 및 피드백을 통해 사이버 위협 분석역량을 강화한다.

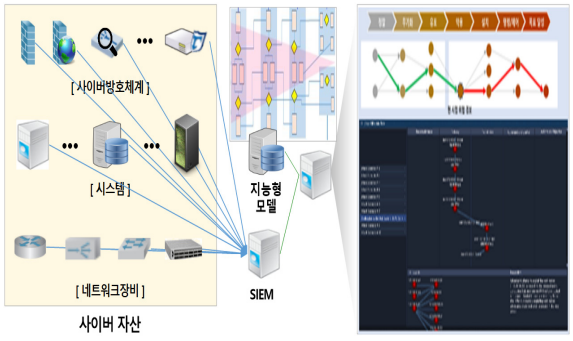

Fig. 5. Configuration of cyber threat alarm analysis system[12]

6. 결 론

본 논문에서는 사이버 공격에 대한 대응역량을 고도화하기 위해 록히드마틴의 사이버 킬 체인과 MITRE ATT&CK 모델을 기반한 사이버 방호기능을 통합 분석하여 선제적으로 사이버 위협을 예측하고, 신속한 결심 및 대응이 가능한 지휘통제를 제안했다.

연관 분석을 통해서는 1개의 공격기술(TTPs)이 2개 이상의 사이버 킬 체인 공격단계에 일부 적용되었고, 또한, 1개의 공격기술(TTPs)에 대응하기 위한 사이버 방호기능은 1개 이상 존재하며, 방어유형과 사이버 방호체계가 다양하게 분포됨을 확인했다.

공격기술(TTPs)에 대응하기 위한 방호기능이 확인되었지만, 사이버 공격은 지능화 · 표적화 · 고도화 · 조직화되어 공격기술(TTPs)이 하루가 다르게 급속도로 발전중이므로 지속적인 국내 · 외 사이버 공격과 위협사례를 분석하여 알려지지 않은 사이버 위협에 대한 방호기능을 확보하여 본 논문에서 제안한 사이버 지휘통제에 연동할 필요가 있다.

향후에는 공격기술(TTPs)에 대해 MITRE가 제안한 방어기능(Mitigation ID)을 기반으로 사이버 킬 체인 공격절차와 방어유형으로 세분화하고 운용중인 방호기능과 연관성 분석을 통해 사이버 방호체계에 대한 방호수준을 제시할 수 있도록 한다.

References

[1] Government of the Republic of Korea, National Cyber Security Master Plan, p. 2, September, 2019.

[2] Seho Choi et al, “A study on Defense Indicators for Evaluation of Defense Cyber Response System,” 2019 KIMST an Academic Conference for Estimating, pp. 646-647, November, 2019.

[3] Kevin Daimi, “Computer and Network Security Essentials,” Springer International Publishing, pp. 585-602, 2018.

[4] Eric M. Hutchins et al, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Proc. 6th ICIW 11 Academic Conferences, Ltd., pp. 113-125, 2010.

[5] U.S. Joint Chief of Staff. Information Operation Doctrine(JP3-13), November, 2012.

[6] The MITRE Corporation, “MITRE ATT&CK,” Accessed Match 21, 2021. https://attack.mitre.org.

[7] Blake E. Storm, Andy Appleaum, Doug P. Miler, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas, “MITRE ATT&CK™ : Design and Philosophy,” MITRE Corporation, June, 2018.

[8] The MITRE Corporation, “MITRE ATT&CK,” Accessed Match 30, 2021. https://attack.mitre.org/resources/updates/.

[9] Jea-woo Yoo, Dae-woo Park, “Cyber Kill Chain Strategy for Hitting Attacker Origin,” Jornal of the Korea Institute of Information and Communication Engineering, Vol. 21, No 11, November, 2019.

[10] Lee, Sun-Jae et al, “A Study on the Analysis and Enhancement for Cyber Security,” The Korea Association For Industrial Security, Vol. 9, No. 1, pp. 69-91, June, 2019.

[11] Korea Information Security Industry Association, 2019, “Survey for Information Security Industry in Korea,” Korea Information Security Industry Association, 9th Floor, 135, Jungdae-ro, Songpa-gu, Seoul, Republic of Korea, pp. 14, 149-158.

[12] Republic of Korea Ministry of National Defense, 2019, “2019 - 2033 Defense Informatization Basic Plan,” Republic of Korea Ministry of National Defense, 22, Itaewon-ro, Yongsan-gu, Seoul, Republic of Korea, pp. 84-88.