사이버전 훈련 평가 지표 수립방안 및 훈련자 훈련 결과 관리 방안

장우현, 김대식*
LIG넥스원, *국방과학연구소
woohyun.jang@lignex1.com, dkim@add.re.kr

Analysis Method of Battle and Trainee Result of Cyber Warfare

Woohyun Jang, *Daesik Kim
LIG Nex1, *Agency of Defense Development

요 약

국가 간 사이버 위협의 심화는 사이버전 훈련의 중요성이 강조되는 계기가 되었다. 사이버전 대비 훈련을 위해서는 실제와 같은 가상공간에서의 모의 전투를 통한 전투 능력 함양이 필수적 이지만, 훈련 결과를 분석하고 평가하는 방안을 마련하는 것 또한 중요한 문제이다. 본 논문에서는 사이버전 모의전투 훈련 이후 훈련에 대한 평가 지표 수립 방안과 훈련자의 능력 향상을 지속 관리하기 위한 평가 항목을 제안한다.

Ⅰ. 서 론

최근 국가 간 사이버 위협 유형이 다양해지고 고도화 되면서 이에 대한 능동적 대응을 위한 전문 인력 양성이 중요해지고 있다. 전문 인력 양성을 위해서는 다양한 교육과 모의전투 훈련이 필요하며 국내·외적인 훈련장 구축 및 훈련체계 확립이 진행 중이다. 사이버 공방능력의 검증을 통한 사이버 역량 강화를 위하여 미 국방부 사이버사령부 주관 사이버 훈련이 있으며 KISA에서는 사이버 훈련장을 구축하여 민간인 대상 대응 훈련을 통한 교육을 통해 인력 양성을 하고 있다.[1][2]

훈련을 통한 전문 전투 능력 함양이 중요하게 대두되고 훈련의 질을 높이기 위한 다양한 시도가 이루어지고 있으나, 훈련 결과를 분석하고 평가하여 훈련자를 관리하고 평가하는 방안에 대한 연구 또한 중요한 문제이다. 본 논문에서는 사이버전 훈련에 대한 평가 지표 수립 방안과 훈련자 결과 관리를 위한 평가 항목을 제안한다.

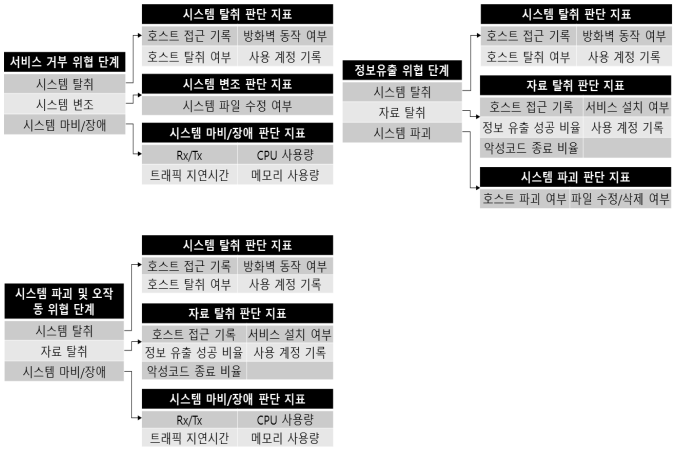
Ⅱ. 본론

훈련은 두 가지 측면에서 평가되어야 한다. 첫 번째는 평가 지표로서 훈련이 이루어지는 가상 전장에서 측정할 수 있는 결과이며 두 번째는 훈련자의 현재 훈련결과를 측정한 것과 과거 대비 얼마나 나아졌는가 하는 것이다. 아래 장절에서는 훈련 목적에 따른 평가지표를 수립하기 위한 방안과 예시를 제시하고 훈련자의 훈련결과 측정 요소를 식별하고 결과 간의 관계를 도출하여 발전되는 훈련 양상을 보일 수 있도록 하는 방법을 제안한다.

1. 평가 지표 수립 방안

훈련 평가 지표는 위협에 따른 대처 결과를 확인해야 하고 위협은 훈련 목적에 따라 다양하게 나타난다. 따라서 [그림1] 과같이 훈련 목적과 위협을 정의하고 그에 맞는 지표를 선정하는 것이 필요하다. 위협의 종류는 다양하지만 크게 서비스 거부 공격 목적, 정보 유출 목적, 시스템 파괴/오작동 목적으로 구분할 수 있으며[3] 각각은 시스템 탈취, 자료 탈취, 시스템 파괴, 시스템 편조, 시스템 마비/장애 등의 단계를 거쳐 작동된다. 위협에 따라 일부 단계는 거치지 않기도 한다.[4] 각 위협에 따라 단계별 시도 행위를 파악하고 각 행위의 결과로서 나타나는 값 또는 그 변화를 분석할 수 있어야 훈련 성공 여부를 판단하기 위한 평가 지표라고 할 수 있다. 각 위협에 따라 수행되는 단계와 단계별 지표는 [그림2]를 통해 알 수 있다.[5][6]

[그림 1] 평가지표 선정 과정



[그림 2] 위협 수행 단계별 평가 지표

각 평가 지표의 정의는 아래 [표1]과 같이 정의한다.

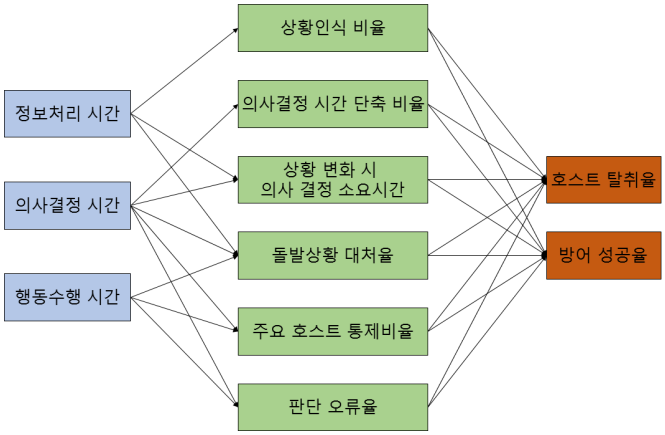
지표 명	지표 정의
호스트 접근 기록	호스트에 비인가 사용자의 접근 기록. Access log 권한 상승 감지된 수
호스트 탈취 여부	위협대상 호스트 대비 탈취성공 호스트 비율
방화벽 동작 여부	방화벽 동작이 감지된 수
사용 계정 기록	계정이 사용된 기록 감지 여부
시스템 파일 수정 여부	호스트의 시스템 파일 수정 감지 여부
정보 유출 성공 비율	전체 주요 정보의 예정되지 않은 복사/전송 비율
악성코드 종료 비율	실행된 악성코드의 수 대비 종료된 악성코드 비율
서비스 설치 여부	예정되지 않은 서비스의 설치 여부
Rx/Tx	시간대별 송수신 트래픽 양
트래픽 지연시간	송수신 트래픽의 지연 시간
CPU 사용량	호스트별 시간대별 전체 CPU용량 대비 사용량 비율
메모리 사용량	호스트별 시간대별 전체 메모리용량 대비 사용량 비율

[표 1] 평가지표 정의

2. 훈련자 결과 평가 항목

훈련의 결과로 나타나는 시스템의 변화를 평가 지표로 정의하였다면 훈련자의 능력에 대한 평가를 수행하여 발전/훈련방향을 제시하여야 효과적인 훈련이 가능하다.[6] 위협을 인식하고 반응하여 조치하는 것이 훈련 과정이며, 이때 인식오류, 잘못된 판단 등을 향상시키는 것이 훈련 목표이다. 훈련 과정이 모여 전체의 인식/조치한 비율 등이 변화되고 결과적으로 작전의 성공여부로 연결된다.[7]

훈련 과정과 결과로부터 최종 작전의 성공여부까지 연관되는 항목들을 다음 [그림3]과 같이 정의하였다.



[그림 3] 훈련자 평가 항목 별 연관관계

각 훈련자 평가 항목은 아래 [표2]와 같이 정의하였다.

훈련자 평가항목	정의
정보처리 시간	공격이 시도된 시각과 훈련자가 공격을 인지한 시각의 시간차
의사결정 시간	훈련자가 공격을 인지한 시각과 조치를 시작한 시각의 시간차
행동수행 시간	훈련자가 조치를 시작한 시각과 조치가 완료된 시각의 시간차
상황인식 비율	실제 공격이 발생한 횟수 대비 훈련자가 인식한 공격 횟수
의사결정 시간	과거 훈련의 의사결정시간 대비 현재 훈련의

훈련자 평가항목	정의
단축 비율	의사결정시간 비율
상황 변화 시 의사 결정 소요시간	국면이 변경된 시각 과 국면이 변경됨을 인지하고 의사결정을 시작한 시각의 시간차
돌발 상황 대처율	훈련 관리자의 돌발 상황에 성공적으로 대처한 비율
주요 호스트 통제비율	훈련시나리오에 설정된 주요 호스트를 점유한 비율
판단 오류율	훈련자가 인식한 공격에 대한 전체 조치사항 중 잘못된 조치사항의 비율
호스트 탈취율	훈련자의 팀에 속한 호스트 중 탈취당한 호스트의 비율
방어 성공률	훈련자가 수행한 모든 훈련의 위협행위를 성공적으로 방어한 비율

[표 2] 훈련자 평가 항목 정의

훈련자의 훈련 결과를 분석하여 부족한 능력을 적합한 훈련을 통해 고도화 함 으로써 향후 훈련의 목표 달성, 높은 평가지표의 달성을 이룰 수 있을 것으로 판단된다.

Ⅲ. 결론

본 논문에서는 훈련에 대한 평가지표를 산출하는 방안으로서 위협의 종류, 단계를 이용하는 방법을 제안하고 그에 따른 지표를 정의하였다. 또한 훈련의 최종 목적인 사이버전에 능숙한 인력 양성을 위해 훈련생의 훈련 이력을 관리하고 능력의 발전을 관리하기 위한 평가 항목을 제안하였다. 제안 방법을 통해 훈련의 목적과 결과를 정량화 하고 훈련자를 지속 관리하여 사이버전 전투원의 능력을 발전시키는데 기여할 수 있을 것으로 기대한다. 향후, 평가 지표 및 평가 항목을 위한 데이터 수집을 고려한 설계, 데이터 수집 및 결과 도출의 자동화가 필요할 것으로 예상된다.

ACKNOWLEDGMENT

이 논문은 국방과학연구소의 지원으로 수행된 연구임(UC180003ED)

참 고 문 헌

[1] ZDNet Korea, 실전 같은 사이버보안훈련장 만들어진다, http://www.zdnet.co.kr/view/?no=20151112170327&re=R_20171130171548

[2] KISA 아카데미, 실전형 사이버보안 전문 인력 양성프로그램, https://academy.kisa.or.kr/edu/planning10.kisa

[3] 사이버위협 시나리오 개발 및 대응방안 연구, 고려대학교 산학협력단, 임종인, 2014년 11월에 완료된 합동참모본부 용역 수행과제

[4] 침해사고 분석 절차 안내서, 한국인터넷진흥원(KISA), 2010.01.

[5] Kyu Sik Yoon, “North Korea`s Cyber warfare the capability and threat,” Military Forum, Vol, 68, pp. 64-95. 2011.

[6] 이윤수, “공격·방어 모의훈련 시스템을 활용한 사이버보안 방어팀 역량 평가모델,” 숭실대학교 대학원 박사학위 논문, 2015.

[7] 김태규 외 4명, “사이버전 전투실험을 위한 공격 및 방어의 효과도 지표에 관한 연구,” 한국시뮬레이션학회 춘계학술대회, 2016.