사이버 훈련에서 방어자 행위 로그 기반 과정 중심 평가 체계 연구

손백한[1], 박기웅[2*]
[1]세종대학교 정보보호학과 석사과정
[2]세종대학교 정보보호학과 교수
baekhan1013@gmail.com, woongbak@sejong.ac.kr

A Process-Oriented Evaluation Framework Based on Defender Behavioral Logs in Cyber Training

Baek-Han Son[1], Ki-Woong Park[2]
[1]Dept. of Computer and Information Security, Sejong University
[2]Dept. of Computer and Information Security, Sejong University

요 약

사이버 위협의 고도화에 따라 조직의 대응 역량 강화를 위한 사이버 훈련의 중요성이 지속적으로 증가하고 있다. 그러나 기존 사이버 훈련 평가는 과제 수행 여부나 FLAG 제출과 같은 결과 중심 지표에 의존하고 있어, 훈련 참여자의 문제 해결 과정과 의사결정 흐름을 충분히 반영하지 못하는 한계를 가진다. 본 연구에서는 이러한 한계를 보완하기 위해 사이버 훈련 환경에서 생성되는 로그 데이터를 방어자의 행위 중심 데이터로 재구성하고, 이를 기반으로 수행 과정을 정량적으로 평가할 수 있는 과정 중심 평가 프레임워크를 제안한다. 제안된 프레임워크는 사이버 공격 대응 과정을 단계별로 구분한 뒤, 각 단계에 대해 신속성, 정확성, 효율성, 영향성의 지표를 적용하는 다차원 평가 구조로 구성된다. 이를 통해 기존의 결과 중심 평가 방식에서 반영하기 어려웠던 수행 과정의 차이를 평가에 포함할 수 있는 가능성을 제시하며, 로그 기반 행동 분석을 평가 체계로 확장하는 방향을 제안한다.

1. 서론

최근 사이버 위협은 특정 시스템에 대한 단순한 기술적 침해를 넘어 민・관・군 전 영역으로 지속 확대되고 있으며 조직의 실전적 사이버 대응 역량 강화를 위한 사이버 훈련의 중요성이 증가하고 있다. 특히 Cyber Defense Exercise(CDX), Capture the Flag(CTF), 공격 및 방어에 대한 유형별 단위훈련과 같은 실습형 훈련은 사이버 훈련장(Cyber Range, 이하 CR)이라는 가상환경을 기반으로 학습자가 탐지・분석・대응・복구 절차에 따라 방어훈련을 직접 수행할 수 있어 실무 역량 향상에 기여한다. 그러나 기존 CR 기반 훈련 평가는 주로 결과 중심으로 이루어져, 학습자가 어떤 과정을 거쳐 대응하고 문제를 해결하였는지를 정밀하게 측정하는데 한계가 있다. 동일한 결과를 도출하더라도 그 과정의 차이는 평가에 반영되지 않으며, 평가 기준의 일관성과 재현성 또한 확보하기 어렵다.

CR 환경에서는 훈련 과정 전반에 걸쳐 다양한 로그 데이터가 생성되며, 학습자가 어떤 명령어를 사용하여 어떠한 순서로 방어를 수행하였는지가 시계열적으로 기록된다. 선행연구에서는 로그 기반 행동 분석이 시도되어 왔으나, 이를 정량적 평가 체계로 확장하는 연구는 부족한 실정이다.

이에 본 연구에서는 CR 환경에서 생성되는 로그 데이터를 행위 중심 데이터로 재구성하고, 이를 기반으로 수행 과정을 정량적으로 평가할 수 있는 과정 중심 평가 프레임워크를 제안한다.

2. 사이버 훈련 및 평가 체계 관련 연구

사이버 훈련은 실제 주요 시설 및 정보체계의 인프라 환경을 모사한 CR에서의 실시간 방어훈련(Cyber Defense Exercise 등), 분야별 보안문제를 해결하는 Capture the Flag(CTF), 그리고 실습 중심의 Hands-on 등 다양한 방식으로 운영되고 있다.

* 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-00438551, 10%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 20%), 대학ICT연구센터(ITRC)(Project No. IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업(Project No. RS-2026-25481431, 30%)의 지원을 받아 수행된 연구임.

2.1. 사이버 훈련 환경 및 국내 연구 동향

국내 연구는 주로 사이버 훈련장의 설계 및 구축에 초점을 두고 진행되어 왔다. 특히 사이버 위기 대응 체계를 반영한 훈련 환경 구성이나 시나리오 기반 훈련 설계에 관한 연구들이 수행되었다[1][2]. 이는 훈련의 현실성과 실무 적용 가능성을 향상시키는 데 기여하였다. 또한 최근에는 실제 사이버 공격 사례를 기반으로 MITRE ATT&CK과 같은 프레임워크를 활용하여 훈련 시나리오를 생성하는 연구도 이루어지고 있다[3].

그러나 기존 연구들은 주로 훈련 환경의 구성 및 시나리오 설계 단계에 집중되어 있으며, 훈련 과정에서 나타나는 학습자의 수행 특성이나 절차적 행동 흐름을 체계적으로 평가하는 방법론으로 확장하는 연구는 아직 초기 단계에 있다. 특히 수행 결과뿐 아니라 방어 과정 자체를 평가 대상으로 포함하는 접근은 상대적으로 부족한 실정이다.

2.2. 로그 기반 행동 분석 및 해외 연구 동향

해외 연구에서는 CR 환경에서 생성되는 로그 데이터를 활용하여 학습자의 행동을 분석하고 수행 과정을 해석하려는 시도가 지속적으로 연구되고 있다. Macak et al.[4]은 프로세스 마이닝(Process Mining) 기법을 활용하여 CTF 유형의 사이버 보안 훈련에서 생성된 이벤트 로그를 분석하고 학습자의 행동 흐름을 프로세스 모델로 추상화하는 방법을 제안하였다. 이를 통해 훈련 참가자 간 행동 패턴의 차이를 시각적으로 비교·분석하고, 이상 행동이나 비효율적 수행 패턴을 식별할 수 있는 가능성을 제시하였다.

또한 learning analytics 기반 연구에서는 훈련과정에서 생성되는 상호작용 로그 및 행동 데이터를 활용하여 학습자의 수행과정을 분석하고 이를 시각화하는 접근이 제안되었다[5]. 이는 학습자의 수행 데이터를 지속적으로 수집·분석하여 훈련 과정에 대한 이해를 지원하고, 학습자의 상태에 따른 적응형 피드백을 제공하는 등 교육·훈련분야의 시사점을 도출하는 데 활용된다.

Amalia Damianou et al.[6]이 제안한 Situational Awareness Scoring System(SASS)은 CR 환경에서 학습자의 상황 인식(SA)을 정량적으로 평가하기 위한 다차원 점수화 프레임워크이다. 해당 연구는 반응 시간, 추론 과정, 도구 활용, 의사결정 결과 등 다양한 행동 및 인지적 지표를 기반으로 이를 정량화하며, 기존의 단순 결과 중심 평가가 아닌 행동 과정과 인지적 요소를 함께 반영한 평가 모델을 제안한다.

그러나 이러한 연구들은 주로 CTF와 같은 실습형 환경에 적용되거나 또는 특정 지표(SA 등) 평가에 초점을 두고 있어, 학습자의 전체 행동 흐름을 반영한 통합적 평가 체계로 확장되는 데에는 제약이 존재한다. 즉, 로그 기반 행동 분석 결과를 종합적인 평가 기준으로 연결하고, 훈련수행 과정 전반을 정량적으로 반영하는 평가 체계는 아직 충분히 정립되지 않은 상황이다.

2.3 기존 연구 분석 및 본 연구의 접근 방향

선행연구를 종합하면, 사이버 훈련 분야에서는 훈련 환경 설계와 로그 기반 행동 분석이 각각 발전하였으나, 이러한 연구들은 개별 영역에 초점을 두고 수행되어, 로그 기반 행동 분석 결과를 실제 평가 체계로 연결하는 데에는 부족한 부분이 존재한다.

이에 본 연구에서는 CR 환경에서 생성되는 행위 로그 데이터를 기반으로 수행 과정을 구조화하고, 단계별 방어 과정과 평가 지표를 결합한 과정 중심 평가 프레임워크를 제안한다.

3. 행위 로그 기반 과정 중심 평가 프레임워크 제안

CR 환경에서 수집되는 행위 로그 데이터를 기반으로 학습자의 수행 과정을 정량적으로 평가하기 위한 프레임워크를 제안한다. 본 프레임워크는 로그 데이터를 행위 단위로 재구성하고, 이를 시간 순서에 따라 행위 시퀀스로 구성한 뒤, 방어 단계별 수행 과정과 평가 지표를 결합하여 학습자의 수행 과정을 정량적으로 평가하는 것을 목표로 한다.

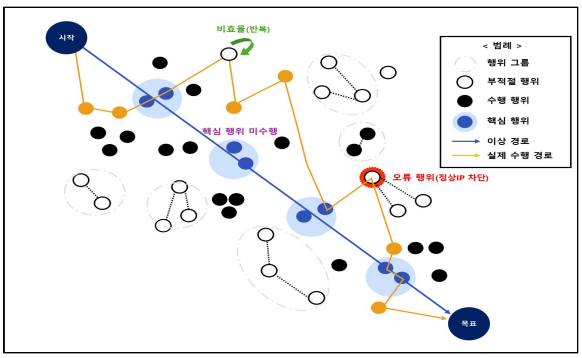

그림1 행위 로그 기반 과정 중심의 평가 프레임워크 개념

[그림1]은 제안하는 평가 프레임워크의 개념을 나

타낸다. 행위 시퀀스는 2차원 공간 상에 표현되며, X축은 방어 단계의 진행도를 나타내며, 시간 순서에 따른 방어 과정의 흐름을 의미한다. Y축은 각 행위의 적합성을 나타내며, 사전에 정의된 이상적인 방어 행위와의 일치 정도를 기준으로 평가된다. 본 연구에서는 이상적인 방어 경로(ideal path)와 실제 수행 경로(actual path) 간의 편차를 분석하여 수행 과정의 품질을 정량적으로 평가한다.

3.1. 행위 로그 데이터 개념 및 구조화

CR 환경에서 생성되는 로그 데이터는 시스템 로그, 방화벽 로그, 사용자 명령어 기록 등 다양한 형태로 존재하며, 이를 그대로 평가에 활용하기에는 해석 및 비교에 한계가 있다. 따라서 본 연구에서는 로그 데이터를 분석 및 평가 가능한 형태로 재구성한다.

명칭	설명
Raw Data (원천 데이터)	시스템/이벤트 로그, 명령어 기록 등 예) sysmon, auth.log, powershell 등
Unit Action (단위 행위)	전처리를 통해 정의된 단위 행위 예) 로그 조회, 프로세스 확인, 파일 삭제 등
Behavior Sequence (행위 시퀀스)	시간 순서에 따라 나열된 단위 행위 집합

표 1. 행위 로그 데이터의 구성

원천 데이터를 정제 및 전처리하여 학습자의 방어 행위 로그 데이터로 변환한다. 불필요한 이벤트를 제거하고, 동일한 의미를 가지는 로그를 통합하여 각 로그를 기능 및 의미 기준으로 단위 행위를 재구성한다. 단위 행위는 로그 데이터를 기반으로 정의되는 최소 단위의 행위이며, 예를 들어 로그 조회, 프로세스 확인, 파일 삭제, 방화벽 정책 적용 등의 형태로 표현된다. 전처리된 행위 로그 데이터는 발생 시점을 기준으로 시간순 정렬되며, 이를 통해 학습자의 방어과정을 나타내는 행위 시퀀스가 구성된다. 이후 단계별 수행 과정 분석 및 평가 지표 산출의 기초 데이터로 활용된다.

3.2. 단계 기반 방어 수행 과정 정의

본 연구에서는 사이버 방어 과정을 NIST SP 800-61(Computer Security Incident Handling Guide)을 기반으로 세분화한다. 각 단계는 요구되는 행위와 의사결정의 성격이 상이하므로, 보다 정밀한 과정 평가를 위해 기존 프레임워크의 “Detection & Analysis” 단계를 분리하고, 각 단계별 행위 특성을 명확히 반영하기 위해 4단계 구조로 세분화하였다.

단계	정의	중요행위
탐지 (Detection)	이상 징후 인지	경보 확인, 로그 모니터링, 이상 트래픽 감지
분석 (Analysis)	공격 의도·범위·영향 파악	공격 분석 및 영향 파악
대응 (Response)	공격 차단·격리	방화벽 차단, 계정 잠금, 시스템 격리
복구 (Recovery)	서비스 및 시스템 정상화	백업 복원, 취약점 패치, 서비스 재개

표 2. NIST SP 800-61 기반 방어 단계 정의

3.3. 과정 중심의 평가 지표 정의

본 연구에서는 수행 과정을 다차원적으로 평가하기 위해 다음과 같은 4가지 핵심 지표를 정의한다.

지표명	정의	수식
신속성 *(Timeliness)*	방어 행위의 소요시간 적절성	$M_T = 1 - \frac{T_{response}}{T_{\max}}$
정확성 *(Accuracy)*	방어 조치의 정확도	$M_A = \frac{N_{correct}}{N_{total}}$
효율성 *(Efficiency)*	방어 수행의 최적성	$M_E = 1 - \frac{N_{unnecessary}}{N_{total}}$
영향성 *(Impact)*	서비스 영향도	$M_I = 1 - \frac{T_{downtime}}{T_{total}}$

- $T_{response}$: 단계별 방어 완료까지 소요된 시간
- $T_{\max}$: 각 단계의 최대 방어 허용 시간
- T_{total} : 전체 훈련 시간 또는 기준 시간
- $N_{correct}$: 올바르게 수행된 행위 수
- N_{total} : 해당 단계에서 수행된 전체 행위 수
- $N_{unnecessary}$: 불필요하거나 비효율적인 행위 수
- $T_{downtime}$: 서비스 중단 시간

표 3. 과정 중심 평가 핵심 지표

평가 지표는 방어 단계별로 적용되며, 각 단계의 수행 특성을 반영하여 과정 중심의 정량적 평가를 가능하게 한다. 탐지·분석 단계는 공격 상황의 인지 및 파악을 목적으로 하며, 해당 단계의 행위는 서비스 중단에 직접적 영향을 미치지 않으므로 영향성 지표는 실질적 대응 행위가 시작되는 대응 단계부터 적용한다.

단계	신속성	정확성	효율성	영향성
탐지 (Detection)	O	O	O	X
분석 (Analysis)	O	O	O	X
대응 (Response)	O	O	O	O
복구 (Recovery)	O	O	O	O

표 4. 단계별 평가지표 구성

3.4. 단계-지표 기반 통합 평가 모델

본 연구에서는 단계와 지표를 결합한 다차원 평가를 위해 다음과 같은 통합 평가 모델을 정의한다.

$$Score = \sum_{s \in S} \sum_{m \in M} w_{s,m} \cdot M_{s,m}$$

- s : 대응단계(탐지,분석,대응,복구)
- m : 평가지표(신속성,정확성,효율성,영향성)
- $M_{s,m}$: 단계s에서 지표m에 대한 평가값
- $w_{s,m}$: 단계s와 지표m에 대한 가중치 ($\Sigma w_{s,m} = 1$)

그림 2. 단계-지표 기반 통합 평가 모델 수식

각 단계의 $M_{s,m}$ 값은 해당 단계에 포함된 행위 시퀀스를 기준으로 산출된다. 방어자의 로그를 기반으로 구성된 행위 시퀀스를 단계별로 분리하여 각 단계에서 수행된 행위를 기준으로 지표 값을 계산하며, 적용 불가 지표는 산출에서 제외한다. 가중치 $w_{s,m}$의 설정은 훈련 목적 및 시나리오 특성에 따라 달라질 수 있으며, 초기 연구 단계에서는 균등 가중치(equal weight)를 기본값으로 적용하되 향후 델파이(Delphi) 기법 또는 계층적 분석(AHP)을 통해 정교화할 수 있다. 해당 모델은 수행 과정의 각 단계에서 다양한 지표를 통합적으로 반영하여, 단일 결과 기반 평가를 넘어 보다 정밀한 평가를 가능하게 한다.

4. 결론 및 향후 연구

본 연구에서는 사이버 훈련 환경에서의 결과 중심 평가 방식이 가지는 한계를 분석하고, 이를 보완하기 위한 행위 로그 기반 과정 중심 평가 프레임워크를 제안하였다. 제안된 프레임워크는 로그 데이터를 행위 단위로 재구성하여 시간 순서 기반의 행위 시퀀스로 표현하고, 방어 단계를 세분화한 후 신속성, 정확성, 효율성, 영향성의 지표를 결합한 "단계 × 지표" 기반 통합 평가 모델을 통해 수행 과정을 정량적으로 평가한다.

이를 통해 동일한 결과를 도출한 경우에도 방어 과정의 차이를 정량적으로 반영할 수 있으며, 기존 결과 중심 평가 방식이 가지는 한계를 보완할 수 있다. 또한 로그 기반 행동 분석을 평가 체계로 확장하고, 수행 과정 전반을 반영한 정량적 평가 구조를 제시하였다는 점에서 의의가 있다.

다만 본 연구는 개념적 프레임워크 제안을 목적으로 하고 있어 실제 훈련 환경에서 수집된 데이터를 활용한 실증적 검증이 이루어지지 않았다는 한계를 가진다. 또한 로그 데이터의 수집 및 표준화 방안, 단계별 지표의 구체적 산출 방법, 가중치 설정의 객관적 기준 마련이 추가적으로 요구된다.

향후 연구에서는 실제 CR 환경 데이터를 기반으로 제안된 평가 모델의 유효성을 검증하고, 단계별 수행 과정과 평가 지표 간의 관계를 정량적으로 분석할 필요가 있다. 이 과정에서 행동 시퀀스 분석, 로그/이벤트 상관관계 분석, 머신러닝 기반 패턴 인식 기법 등을 적용하여 평가 모델의 자동화 및 고도화를 추진하고, 델파이(Delphi) 기법이나 계층적 분석(AHP)을 통한 가중치 정교화, 그리고 다양한 훈련 시나리오에 적용 가능한 범용 평가 체계 구축을 통해 사이버 훈련 평가의 표준화 및 실무 적용 가능성을 확보하는 방향으로 연구가 확장될 필요가 있다.

참고문헌

[1] 유재학 외, "지능형 사이버 훈련장의 기술 동향", 전자통신동향분석, 제37권 제4호, pp. 36-45, 2022

[2] 최영한 외, 사이버위기 경보 기반 사이버 방어 훈련장 설계 및 구축 연구, 정보보호학회, 제30권 제5호, 2020. 10, pp. 805-821.

[3] 홍수연 외, "사이버전 훈련을 위한 ATT&CK 기반 모의 위협 발생기 설계 및 구현", 한국군사과학술학회지, 제22권 제6호, 2019, pp.797-805

[4] Martin Macak, et al, "Process Mining Analysis of Puzzle-Based Cybersecurity Training", Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE), pp. 449-455, 2022

[5] Pantaleone Nespoli. et al, "SCORPION Cyber Range: Fully Customizable Cyberexercises, Gamification and Learning Analytics to Train Cybersecurity Competencies", Human-centric Computing and Information Sciences(HCIS), Vol. 15, pp. 1-25, 2025

[6] Amalia Damianou, et al, "Measuring the unseen: a situational awareness scoring framework for cyber range training", International Journal of Information Security, Vol. 25, No. 2, 2026