시스템 이벤트 데이터셋에 대한 시나리오 기반 위험수준 라벨링

강재현*, 유영록**, 김민수* (교신저자)

*목포대학교, **(주)소울소프트

s193911@365.mokpo.ac.kr, young-rok.yu@soulsoft.co.kr, phoenix@mokpo.ac.kr

Scenario-based Risk Labeling of System Event Datasets

JaeHyun Kang*, Young-Rok Yu**, Minsoo Kim*

*Mokpo National University, **Soulsoft

요 약

여러 시스템을 운용하는 기업망에서는 수많은 이벤트 로그를 수집할 수 있다. 이러한 데이터는 인공지능 기술에 활용 가능한 데이터셋으로 구축할 수 있다. 특히 지도학습을 위해서는 데이터에 대한 라벨링이 필수적이다. 본 논문에서는 시나리오 기반으로 데이터셋에 대한 라벨링 방법을 제안하였다. 시나리오에 대하여 지표 유효 수준과 업부 정상 수준을 부여하여 시나리오에 대한 위험성을 분류할 수 있도록 하였다. 이러한 라벨링 방법은 다양한 산업체와 시스템에서 경험적 지식과 전문가 평가에 따라 그 수준을 분류할 수 있을 것이다.

Ⅰ. 서 론

현재 인공지능 기술은 다양한 분야에서 활용되고 있다. 특히 빅데이터를 활용하여 학습을 수행하고 의미있는 판단을 내릴 수 있다. 산업제어망에서 활용가능한 공개된 데이터셋으로 인공지능 기술을 적용하는 연구도 진행되고 있다. 그러나, 산업체마다 시스템에서 발생하는 정보는 매우 다양하다. 그래서 산업체에서는 기업망이나 시스템에서의 행위를 모니터링하고 이상 징후를 탐지하기 위해서 자체적으로 수집된 데이터셋을 활용하기도 한다.

공개된 데이터셋은 공격행위를 시뮬레이션하여 수집된 것으로 라벨링(labeling)이 되어 있다. 그러나 산업체에서 자체적으로 수집한 데이터셋은 정상적인 활동을 기록한 것이 대부분이다. 따라서 이러한 데이터셋에 공격행위를 라벨링 할 수 없다. 본 논문에서는 산업체 업무망에서 수집된 데이터셋에 위험 수준에 따라 라벨링 하는 방법을 연구하였다.

Ⅱ. 본론

가. 데이터셋 활용 기술

기존 시스템에서 발생한 로그 데이터를 기반으로 정보 유출이나 비정상적인 활동을 탐지하기 위해서는 앞에서 언급한 데이터셋 관련 인공지능 기술이 필요하다. 산업체에서는 보안 접점 강화를 위해서 업무망과 인터넷망을 분리하여 운영하고 있다. 기업에서는 정보 유출을 방지하고 업무 정보는 열람이 가능한 환경을 고려한다. 따라서 기업망에서의 보안 위험성을 진단하고 탐지하기 위해서는 기업에서 활용되는 데이터를 기반으로 판단이 이루어져야 한다.

인공지능 기술은 여러 분야에 적용되고 있다. 산업제어시스템이나 기업망에서의 이상징후를 탐지하기 위한 환경에서도 인공기술이 활용하는 방안이 연구되고 있다. 이러한 연구를 위하여 공개된 데이터셋을 활용하고 있다. 이러한 데이터셋에 인공지능 모델을 적용하기 위해서는 몇 가지 작업이 필요하다. 그 내용은 다음 표 1과 같다[1]. 이 중에서 가장 먼저 이루어져야 하는 작업은 라벨링이다.

[표 1] 데이터셋에 인공지능 기술 적용 방법

스킬	설명
라벨링	데이터에 의미를 부여하는 것으로 이진 또는 다중 클래스로 레이블 생성함
벡터화	다양한 벡터화 알고리즘 사용하여 데이터를 인코딩하거나 데이터 사이의 관계를 표현함
언어 모델	언어모델 BERT를 사용하여 시스템이나 네트워크 이벤트 데이터를 사전학습 수행
강화학습	다양한 변종을 탐지하기 위해 강화학습 알고리즘 등을 적용
다차원 분석	통계값, 이상 값 등의 다양한 척도로 분석

기업망에서 행위 위험도는 핵심위험지표(KRI, Key Performance Indicator)로 수치화 한다[2]. 이러한 지표를 설정하기 위해서는 기업망에서 수집된 데이터에 라벨링이 필요하다. 데이터셋에서 여러 이벤트를 행위 별로 분류할 수 있고, 공격행위를 구분할 수도 있다. 그러나 무작위로 수집된 데이터셋의 경우 이러한 라벨링을 수행하기 어렵다.

나. 시나리오 기반 위험도 표현

기존 시스템이 행위자의 시스템 로그에서 이벤트를 활용했다면, 오직 서버 로그만을 활용해야 하므로, 이에 상응하는 특징 공학 기술 개발 필요하다. 더구나 기존 시스템 로그 데이터에서는 정보 유출 사고를 찾기 어렵기 때문에 비정상 데이터를 수집하고 라벨링의 어려움이 존재한다. 이러한 문제를 해결하기 위해서는 시스템에서의 행위 로그를 시나리오 기반으로 정의하고 위험도를 표현하는 방법을 생각할 수 있다. 표 2에서는 자료전송 시스템에서의 시나리오를 분류하였다. 표에서는 A사의 파일전송 보안 시스템에서 발생시키는 로그 이벤트 타입을 관련된 시나리오에 매핑시켰다.

기업망에서 정보유출 시나리오에 근거하여 침투 단계별로 위험도를 설정할 수 있다. 최초 침투 단계에서는 인증 및 접속 시스템에 대한 모니터링이 필요하다. 첫 인증에서 생체 인증을 사용한다면, 인증 처리 정보가 있다. 원격 근무 시스템의 경우 접속 단말 정보와 사전 승인 정보가 있다. 빅데이터 기반으로 직원 계정의 활동 이력을 추적한 결과도 포함된다.

내부망 침투 단계에서 중요 서버에 대한 접속 정보를 모니터링하는 것도 필요하다. 주 접속 계정과 시스템 정보 등을 바탕으로 비정상적인 이용

[표 2] 자료전송 시스템 시나리오의 지표 가중치와 관련된 이벤트 타입

연번	시나리오	지표 유효성	업무 정상성	파일전송 시스템 이벤트
1	허용되지 않은 파일 유형 전송	2	2	PV_NOT_ALLOWED_FILE
2	개인정보 탐지를 지원하지 않는 형식 전송	1	2	PV_PRIVATE_SKIP_UNKNOWN, PV_PRIVATE_INFO_FILE PV_CLIPBOARD_PRIVATE_INFO, AC_PERSONAL_INFO_FILE_CANCEL
3	요청 파일과 업로드 파일의 포맷 불일치	3	3	PV_NO_MATCH_FILE
4	파일 검사 예외요청	2	2	PV_INTEGRITY_ENCRYPT_SKIP
5	탐지 예외요청을 한 경우	2	2	PV_EXEMPTION_APT_EXCEPTION, PV_APT_EXCEPTION, PV_VACCINE_EXCEPT
6	예외 처리로 결재를 거치지 않음	2	2	PV_ENCRYPTED_FILE_SKIP, AC_APPROVAL_EXCEPTION
7	자료 전송 시, 악성파일로 탐지되어 차단	3	3	PV_MALICIOUS_FILE, EV_FALE_POSITIVE_APPROVAL_FILE
8	자료 전송 시, 파일이 암호화되어 차단	1	2	PV_ENCRYPTED_FILE
9	암호화된 파일 다운로드	1	1	AC_ENC_FILE_DOWNLOAD
10	파일 내부 용량 초과	1	2	PV_NOT_ALLOWED_ZIP_ENTRY_SIZE
11	무결성 검증에 따라 위변조된 클라이언트 패치 파일	3	3	AC_CLIENT_PATCH_FILE_FORGE, EV_CLIEENT_INTEGRITY_FAIL
12	미등록/휴면 계정에 의한 자료 전송 시도	1	2	AC_DORMANT_ACCOUNT_LOGIN, AC_NOT_REGIST_USER_LOCK
13	미등록/휴면 계정으로 로그인	2	3	AC_DORMANT_ACCOUNT_LOGIN, AC_NOT_REGIST_LOGIN_FAIL

내역을 기록할 수 있다. 내부망에 위협적인 악성코드 설치나 로그 삭제 등의 행위와 같이 위험 수준이 높은 행위가 있다. 내부 데이터의 유출 행위는 상시 모니터링을 통해서 정보를 수집한다. 데이터 전송이 이루어진다면, 데이터의 용량, 빈번도, 승인 여부에 대한 로그를 검토할 수 있다.

다. 가중치 설정

기업망에서의 행위는 행위의 목적과 위험도에 따라 라벨링을 할 수 있다. 내부자의 계정 도용, 중요 정보에 대한 접근, 승인되지 않는 행위 수행 등의 위험도가 높은 행위에 대하여 위험 수준 부여한다. 이는 침투 행위의 목적에 따라 그 수준과 가중치를 부여할 수 있다. 또한 알려지지 않은 공격 시나리오에 대응하기 위한 방법도 필요하다. 이 경우에는 정상행위 데이터에 대한 라벨링을 수행할 수 있다. 정보 접근 행위에 대하여 계정, IP, 접근 허용 여부 등에 따라 점수(score)를 다르게 적용할 수도 있다.

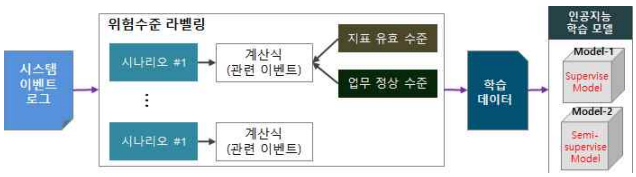
표 2에서는 파일 전송에 대한 위협 시나리오를 정의하고 그 가중치를 설정하였다. 가중치 값은 기업에 대한 정보유출 사건의 경험적 지식을 기반으로 작성되었다. 표에서는 A사의 파일전송 보안 시스템에서 발생시키는 로그 이벤트 타입을 관련된 시나리오에 매핑시켰다.

[표 3] 지표의 근거

레벨	지표 유효 수준	업무 정상 수준
1	해당 행위의 위험도는 낮음	해당 행위로 인한 업무 장애는 거의 없음
2	해당 행위는 잠재적인 위험 가능성이 있음	해당 행위가 발생하였을 때, 업무에 지장을 줄 수 있음
3	해당 행위의 위험도가 매우 높음	해당 행위가 발생하였을 때, 업무 장애가 불가피함

표 3에서는 지표 유효 수준과 업무 정상 수준에 대한 레벨별 의미를 설명하고 있다. 데이터 품질관리를 위해서는 여러 가지 지표가 필요하다[3]. 가중치는 지표 유효 수준과 업무 정상 수준을 1레벨에서 3레벨로 구분하였다. 지표 유효 수준은 해당 행위가 주는 영향력을 바탕으로 타당성을 의미한다. 업무 정상 수준은 해당 지표가 지켜지지 않을 경우 업무에 영향을 주는 정도를 의미한다. 표 2의 가중치 값은 기업에 대한 정보유출 사건의 경험적 지식을 기반으로 작성되었다.

라. 학습모델에 적용



<그림 1> 위험수준 라벨링 적용 모델

기업망에서 시스템 로그는 위험수준 라벨링을 통하여 정련된 학습 데이터셋으로 구축할 수 있다. 이러한 데이터셋은 여러 가지 인공지능 학습모델에서 활용할 수 있게 된다.

Ⅲ. 결론

기업망의 시스템에서는 수많은 이벤트 로그가 발생한다. 이러한 로그는 정보유출과 보안을 위한 데이터셋으로 사용할 수 있다. 데이터셋을 인공지능 학습 모델로 활용하기 위해서 첫 번째로 데이터 라벨링이 필요하다. 본 논문에서는 시나리오 기반으로 데이터셋에 대한 라벨링 방법을 제안하였다. 시나리오에 대하여 지표 유효 수준과 업부 정상 수준을 부여하여 시나리오에 대한 위험성을 분류할 수 있도록 하였다. 이러한 라벨링 방법은 다양한 산업체와 시스템에서 경험적 지식과 전문가 평가에 따라 그 수준을 분류할 수 있을 것이다.

ACKNOWLEDGMENT

본 과제(결과물)는 2022년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다. (2021RIS-002)

참 고 문 헌

[1] 신경아 이윤호, 배병주, 이수항, 홍희주, 최영진, 이상진, “악성코드 대응을 위한 신뢰할 수 있는 AI 프레임워크,” 한국정보보호학회 논문지, 제32권 제5호, 2022년

[2] 전상미, “IT 위험 정량화로 효율적 위험관리 달성,” 데이터넷, 2008년 https://www.datanet.co.kr/news/articleView.html?idxno=40667

[3] 한국지능정보사회진흥원, *제1권 품질관리 안내서*, 인공지능 학습용 데이터 품질관리 가이드라인 v2.0, 2022년