보안이벤트 자동 검증 방법 및 장치

KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr

특 허 명 보안이벤트 자동 검증 방법 및 장치

Keyword 빅데이터, 개인정보, 사이버보안, 보안장비

발 명 자 김용인 / 지관영

기 술 성

기술 개요

- 본 특허는 보안이벤트를 자동 검증하는 방법 및 장치에 관한 기술임

기존 기술 문제점

- 종래의 연구는 보안이벤트에 대한 기본 정보 (IP, 포트, 프로토콜, 이벤트 명 등)만을 이용하여 사이버 위협 동향 파악 및 대상 보안이벤트 수를 감소시키기 위한 간접적 접근에 초점을 맞추고 있어, 보안이벤트에 대한 실제 해킹공격 발생여부를 판단하기 어려우며, 보안 관제 업무 수행 시 추가적인 분석이 필요함
- 기존 연구는 대용량 보안이벤트에 대한 자동 분석을 위해 주로 데이터 마이닝 및 기계 학습 기술을 적용하고 있으나, 이러한 접근 방식은 정확도가 떨어지는 문제점이 존재함

기술의 특징 및 우수성

▶ 기술의 특징

- 탐지규칙 기반 보안장비 (IDS/IPS, TMS 등)에서 공격으로 탐지된 보안이벤트의 특성을 추출하는 방법을 제공
- 탐지규칙 기반 보안장비에서 공격으로 탐지된 보안이벤트를 공격 유형에 따라 분류하는 방법을 제공
- 각 공격 유형에 따른 알고리즘을 적용하여 보안이벤트를 자동 검증하는 방법을 제공

▶ 기술의 우수성

- 보안장비 탐지규칙 기반 보안장비가 탐지한 보안이벤트를 자동으로 검증하여 정탐(실제 공격에 의해 발생한 보안이벤트)과 오탐(정상 통신에 의해 발생한 보안이벤트)으로 판별함으로써 해당 보안장비의 효율성을 극대화함
- 탐지 패턴을 우회하는 신종 또는 변종 공격이 증가하고, 탐지 패턴이 없는 알려진 공격에도 대응
- 대용량 사이버 공격에 대해 직관적으로 인지할 수 있는 효과가 있음
- 각 공격 유형에 따른 알고리즘을 적용하여 높은 수준의 자동 검증 결과를 도출함

보안이벤트 자동 검증 방법 및 장치

상세설명

- 본 기술의 보안이벤트 자동 검증 방법은 보안이벤트 및 보안이벤트와 관련된 정보를 입력, 특성 추출, 분류 및 검증하는 단계를 포함
- 보안이벤트 자동 검증 장치는 보안이벤트들의 자동 검증을 위하여 먼저 기본 정보, 정적 요소 및 동적 요소를 추출함
- 과학 기술 사이버 안전 센터 (S&T-SEC)에서 구축 및 운용 중인 침해 위협 관리시스템(TMS)을 활용하여 임계치 기반으로 사고 처리한 보안이벤트의 특성을 통계적으로 분석/분류하여 보안이벤트 탐지 결과가 정탐/오탐 여부 판별
- 사이버 공격의 유형 예시 (악성 URL, 악성코드, 다운로드, 악성코드 감염, 정보 전송, 파일 업로드) 및 동적 특징 정보를 활용하여 자동 검증함

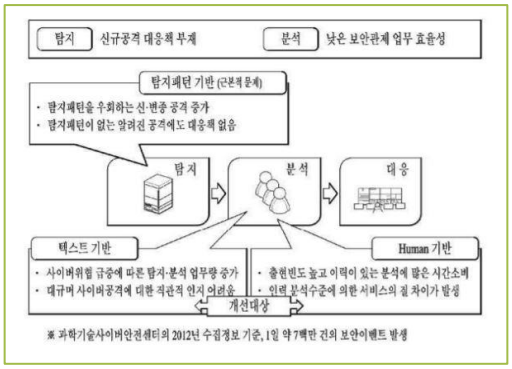


그림1 종래 탐지 패턴 기반의 보안 관제

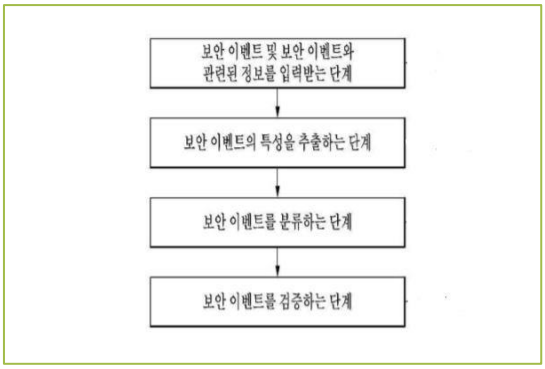


그림2 보안이벤트 자동 검증 방법

기술완성도 (TRL)

기술완성도 : TRL0

TRL1	TRL2	TRL3	TRL4	TRL5	TRL6	TRL7	TRL8	TRL9
기술원리 발표	기술컨셉 설정	기술컨셉 증명	Lab Scale 시제품개발	Full Scale 시제품개발	구현환경 적용실험	유사 상용품 개발	상용품 완성	상용품 실시

활 용 분 야

활용분야 및 적용제품

활용분야

- ◆ 보안관제/ 보안 컨설팅 분야
- ◆ 클라우드 보안관제 분야

적용제품

- ◆ Remote/On-site 관제 프로그램
- ◆ 개인정보보호체계 수립 컨설팅 프로그램

보안이벤트 자동 검증 방법 및 장치

산업동향(기술 동향 및 트랜드 등)

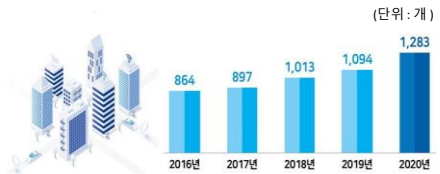
- 빅데이터 시장이 커짐에 따라 데이터에 대한 보안의 중요성도 함께 강조됨
- 보안관제서비스를 통해 기술지원 역량과 안정된 인프라를 구축 및 운영 지원
- 보안컨설팅을 통해 IT자산에 일어날 수 있는 위험을 분석, 이에 대한 대책을 수립하고 실천하도록 지원하는 자문 서비스 제공
- AI기술을 접목한 보안관제침해대응 자동화 플랫폼, 여러 인프라 산업 시설들을 통합적으로 제어하는 산업제어시스템 보안컨설팅 시스템, 스마트팩토리 보안컨설팅 서비스 등 정보보안관련 신규 사업사업 확대 전망

시장전망(목표시장 규모 및 전망)

- 4차 산업혁명과 코로나-19로 인해 언택트 및 온택트가 강조되는 시기가 더욱 앞당겨졌고, 이 때문에 온라인으로 흘러 들어오는 전세계 연간 데이터 총량은 막대한 증가세
- 국내 정보 보안시장은 2019년에는 약 3.2조원의 규모로, 매년 연평균 약 10.6%의 성장률로 성장했고, 앞으로도 계속해서 성장할 것으로 전망
- 국내 정보보호기업은 1,283개로 전년도, 1,094개보다 약 17.3% 증가로 조사
- 디지털경제 가속화로 정보보호에 대한 시장 수요 및 중요성이 상승함에 따라 정보보호기업
- 수는 꾸준히 증가하여 연평균 10.4% 성장율을 보임
- 국내 정보보호산업의 매출 규모는 전년 대비 6.4% 증가 (출처 : IDC, 과학기술정보부, 한국정보보호산업협회)

출처 : 한국 인터넷진흥원

그림3 국내 정보 보안 시장 규모



출처 : 과학기술정보부/한국정보보호산업협회

그림4 연도별 정보보호 기업 수

지재권현황

권리현황	특허출원번호	발명의 명칭
출원	10-2016-0017262	보안이벤트자동검증방법및장치

문 의 처

기술이전

KiSTi www.kisti.re.kr 한국과학기술정보연구원 Korea Institute of Science and Technology Information

담 당 자 심원보
연 락 처 042-869-0911
이 메 일 wbsim@kisti.re.kr

기술문의

KiSTi www.kisti.re.kr 한국과학기술정보연구원 Korea Institute of Science and Technology Information

담 당 자 심원보
연 락 처 042-869-0911
이 메 일 wbsim@kisti.re.kr