144

기술 분류_ 사이버보안

사이버공격 실시간 추적 가시화 기술

01 기술 개요

IP주소에 대한 공격(이상행위)을 실시간 및 통계적으로 가시화함으로써 사이버공격의 근원지와 구조등을 직관적으로 분석할 수 있는 환경을 제공하는 가시화 시스템에 관한 기술

기존의 보안 이벤트(IP주소, 포트, 프로토콜 등) 기술은 중점적으로 모니터링할 공격자 IP를 선정할 수 있는 기술적 부재 존재. 가시화 시스템 기술로 신·변종 사이버 위협의 탐지와 이상 행위의 3차원 그래픽 정보 제공 및 기존 정보와의 상관관계를 분석, 제공함 으로써 사이버 위협 탐지 업무 수행이 가능함

[대표도면]

02 기술 차별성

실시간 및 통계적 가시화에 기반한 모든 IP의 실제 공격행위 여부를 직관적으로 탐지 및 분석하여 업무효율성을 높일수 있음

- 침해위협관리시스템(TMS)과 침입탐지방지시스템(IDS·IPS)등을 탐지한 보안로그를 실시간으로 처리할 수 있음
- 공격자 상관정보 가시화 기술은 IP들간의 상호관계를 가시적으로 표현하여 잠재적 위협분석 및 추가 공격확산·전파를 선제적으로 대응할 수 있음

이상행위를 수집하기 위해 대용량 보안정보를 장시간 수집하고 다양한 정보를 조합하여 가시화 가능

- 사이버 보안 정보 가시화 장치, 사이버 보안 정보 가시화 방법 및 사이버 보안 정보를 가시화 하는 프로그램을 저장하는 저장매체를 제공함
- 공격자상관정보 가시화장치는 IP간의 연관관계를 가시화하여 공격발원지·근원지를 추적함으로써 해킹공격을 원천적으로 차단할수있음

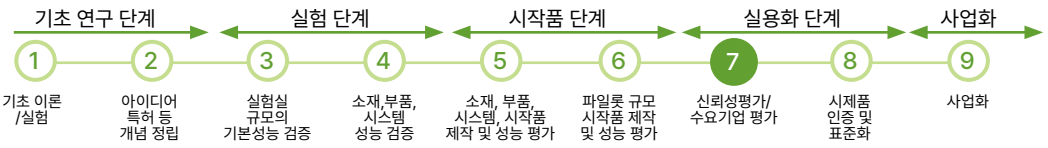
내·외부 공격자 가시화는 24시간 동안 실시간으로 공격행위를 추적 및 분석하여 시각화

- 전처리 모듈은 스토리지부터 IP주소 등의 출발지 및 목적지 정보, 발생시간등이 포함되어 있는 보안이벤트를 수신하여 정보를 추출하고, 통계정보 모듈은 보안이벤트 대상기관의 내·외부 공격자 IP 주소의 구분 등에 관한 통계 정보를 생성
- 가시화 모듈은 보안이벤트의 공격행위를 확인하는 방법으로 내·외부 공격자 및 공격자 상관정보 가시화 기술로 분류 할 수 있음

03 기술 키워드

보안솔루션, IDS, IPS

04 기술의 TRL 단계



144

기술 분류_ 사이버보안

사이버공격 실시간 추적 가시화 기술

05 사업화 포인트

인공지능은 기술의 발전과 변화속도가 매우 빠르고, 기술완성도가 7단계(유사 상용품 개발)이기 때문에 기업 및 시장 환경에 맞는 최적화를 통한 상용품 제작 후 신속한 시장 진입 전략 수립 필요

06 활용 분야 및 시장 규모

활용 분야

네트워크보안 시스템, 시스템보안솔루션

시장 규모 및 전망

금융위원회가 21년 2월 우리은행 등 28개사에 Mydata 관련 사업을 허가했고, 과기부 등에 따르면, 국내 데이터 산업 시장 규모는 2020년 19조 수준에서 Mydata 시장 개방으로 2023년 30조 규모로 성장할 것으로 전망됨

(출처:아시아투데이)

API 사업은 금융권에서 시작되어 타 산업으로 확대되고, API Management를 활용한 Open API 플랫폼이 향후 기업에게 디지털 비즈니스 플랫폼으로써 역할을 해줄 것으로 예상. 또한, Mydata(본인정보활용) 시장 선점을 위해 경쟁이 가속화되고있음

(출처:아시아투데이)

07 지식재산권 현황

권리현황

특허명	공격자 가시화 장치 및 공격자 가시화 장치의 동작 방법
출원번호	10-2018-0142167
권리자	한국과학기술정보연구원
관리기관	한국과학기술정보연구원
담당자	주용하
문의처	042-869-0977