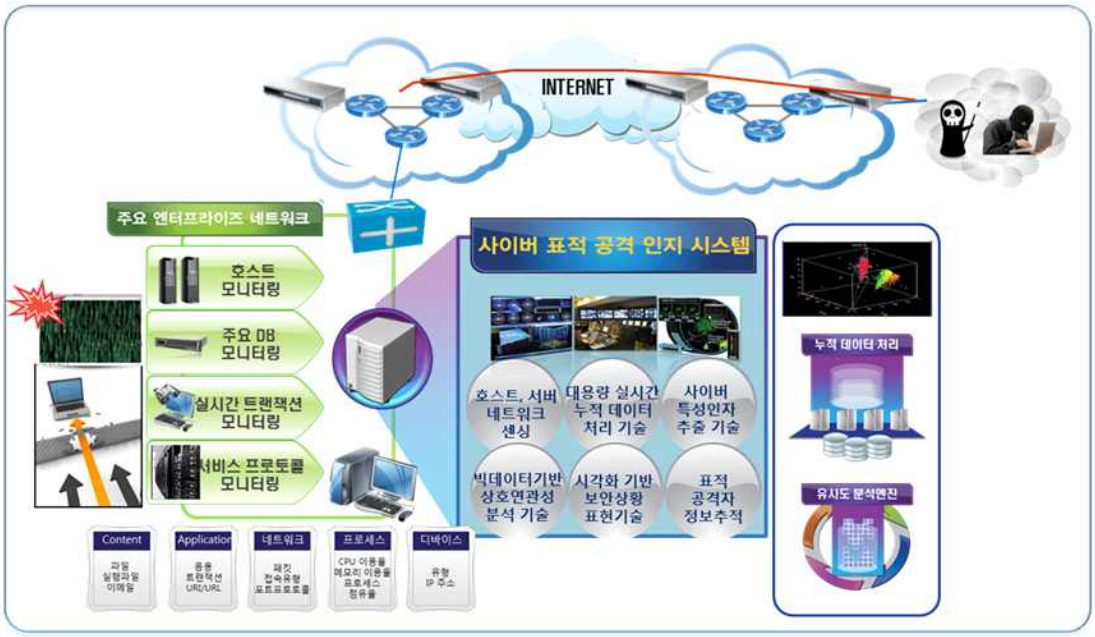
빅데이터 분석기반 지능형 사이버 공격 인지 및 추적기술

한줄설명	주요 IT기반 시설에 대한 사이버테러 수준의 표적공격 사전인지와 공격 근원지 추적을 목표로 하는 지능형 사이버 보안기술
성과개요	사이버 표적 공격(APT)과 같은 알려지지 않은 치명적 공격에 대응하기 위해서는 주요 IT기반 시스템의 네트워크, 시스템, 응용서비스 등에서 발생하는 데이터 및 보안이벤트의 연관성을 분석하고 공격자의 근원지를 추적할 수 있는 지능형 보안(Security Intelligence)을 지향하는 차세대 보안정보 분석 기술 확보
성과 개념도	
성과 우수성	**o 신종·변종 악성코드 탐지를 위한 호스트 이상 행위 탐지 엔진개발 (SINBAPT-SigFree AV)** – 마이닝기반 이상행위 동적 분석 알고리즘 확보(신종 악성코드 진단율 국내 최고 알고리즘) – 호스트 행위기반 악성코드 탐지 엔진 시험결과 세계 최고 수준 : 탐지율(96.9%), 오탐율(4.6%) **o 사이버게놈 분석기반 알고리즘 개발(SINBAPT-Gene): 표적공격 특성인자 DNA 모델링** – 사이버게놈 모델 악성코드 프로파일링 : 유사도 분석 탐지율 : 93.59%, 오탐율 4.04% **o 해킹 경유지/공격지 역추적 알고리즘 세계최초 개발(통신 3사(KT, SKBB, LGU+) 및 해외 사이트 연동 시험 완료** – xFlow 정보기반 역추적 알고리즘(세계 최초 해킹 공격자 경유지, 근원지 추적 알고리즘) – KT KORNET 상용망 역추적 시스템 시험 서비스 (혜화전화국, 국제 관문 노드)
활용 분야	o (응용 및 확장성) 호스트PC에서 발생하는 행위이벤트 데이터 분석을 위한 데이터마이닝 기술 확보는 보안로그 빅데이터를 분석하는 SIEM 시장으로 사업영역 확대 예상 o 컴퓨터 바이러스 백신분야 세계 선도기업과 차별화된 기술력으로 경쟁력 확보 및 기술 의존도 감소 o 지능화, 고도화되는 보안 위협에 대응하는 지능형 보안 시스템 구축을 위한 빅데이터 활용 분야의 하나로사이버 보안기술의 고도화 기술로 활용

파급 효과	o SIEM시장은 로그관리 외에도 통합모니터링/접속관리 등으로의 활용 영역 확대로 보안 플랫폼 개발(보안/운용/어플리케이션 분석)을 통한 통합보안관제 분야 활용 가능 o 공격자 경유지/근원지 추적 핵심기술 기반 역추적을 위한 서비스 및 비즈니스 모델 창출 o 데이터 마이닝 기반의 알려지지 않은 신종/변종 악성코드 탐지 기술 확보로 세계시장 점유율 향상 기대(국내 기업의 세계시장 점유율은 2% 이하) o 네트워크 안정성 확보로 국가적 이슈인 사이버 표적 공격에 대응하여 경제적, 사회적 피해 최소화 o 사용자/기업이 안심하고 서비스를 이용/제공하는 인터넷 망 환경조성과 사이버 공격에 따른 국가인터넷 서비스 장애에 대한 불안감 해소

소속 : SW·콘텐츠연구소 사이버보안연구본부 사이버보안시스템연구부 네트워크보안연구실 / 성명 : 김익균
연락처 : 042-860-5442 / E-Mail : ikkim21@etri.re.kr