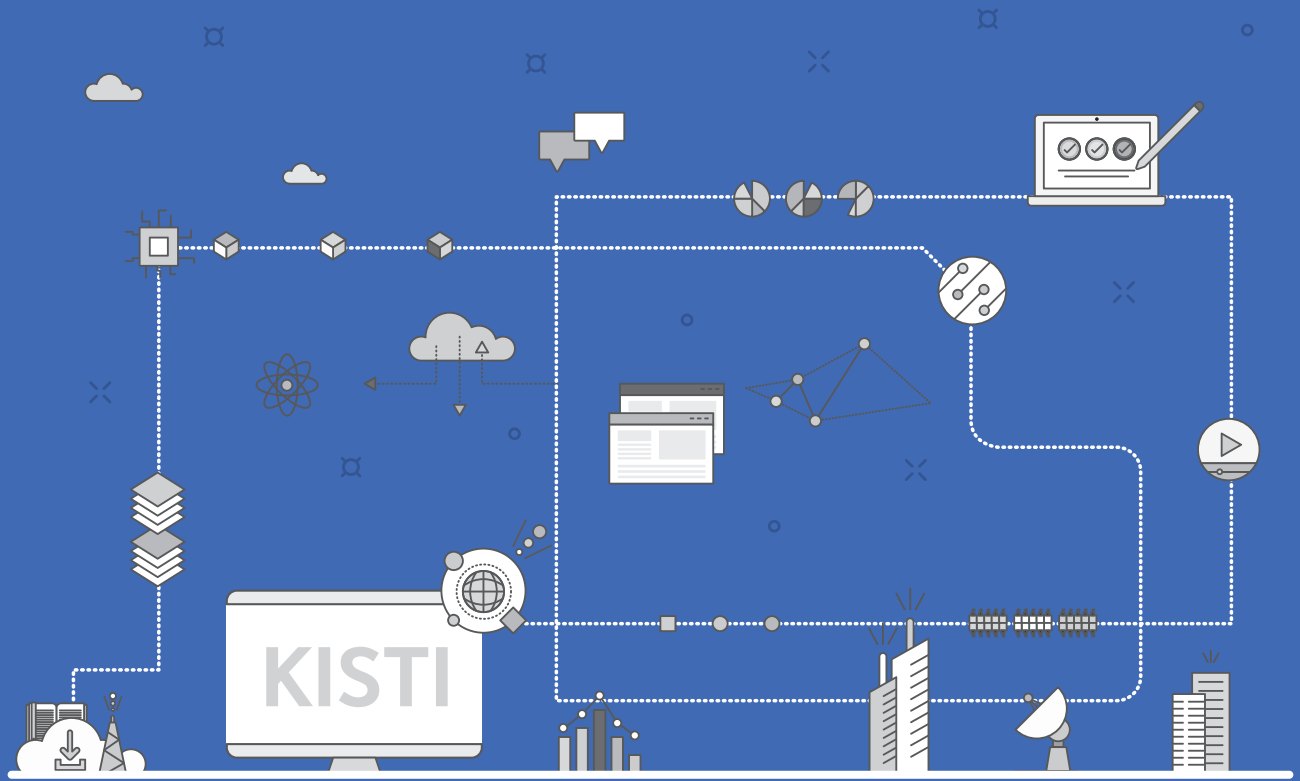
국가슈퍼컴퓨팅본부

자동분석 기반
통합보안정보분석시스템(SMARTer)



Keyword 사이버 해킹, 실시간 탐지, 자동분석, 보안관제, 첨단연구망, 실시간 보안관제

연구책임자 최장원

기술개요

탐지된 대용량 보안이벤트(사이버 공격)에 대해 공격 유형별 자동 검증 알고리즘을 기반으로 정탐/오탐 여부를 신속하게 자동 검증함으로써 실시간으로 보안관제가 가능하도록 한 기술임

기존 기술의 문제점

탐지 패턴을 기반으로 탐지하기 때문에, 탐지 패턴을 우회하는 신종 또는 변종 공격 및 탐지 패턴이 없는 공격에는 대응할 수 없음

텍스트를 기반으로 보안이벤트를 분석하기 때문에, 대용량 사이버 공격에 대해 직관적으로 인지하기 어려움

사람이 보안 관제를 하기 때문에, 개인별 분석 수준에 따른 서비스 질의 차이가 발생함

기술 내용 및 차별성

대용량 보안이벤트에 대한 신속하고 정확한 자동 검증 가능

기술 내용

- 자동분석 기반 통합보안정보분석시스템
  - 탐지규칙 기반 보안장비(IDS/IPS, TMS 등)에 의해 공격으로 탐지된 보안이벤트를 정탐* 및 오탐*으로자동 검증함
    *정탐 : 실제 공격에 의해 발생한 보안이벤트
    *오탐 : 정상 통신에 의해 발생한 보안이벤트
- 탐지된 보안이벤트를 시그니처 기반의 보안이벤트*와 임계치 기반의 보안이벤트*로 분류하여 6가지 유형별 자동 검증 알고리즘을 적용함
  - 유형 : 악성 URL, 악성코드 다운로드, 정보 전송, 파일 업로드, 악성코드 감염, 임계치 기반 보안이벤트
    *시그니처 기반의 보안이벤트 : 설정된 특정 문자열을 포함하는 보안이벤트
    *임계치 기반의 보안이벤트 : 설정된 임계치를 초과하여 발생한 보안이벤트

차별성

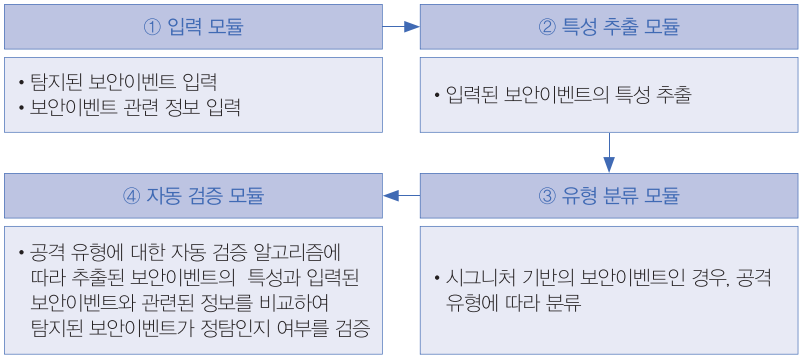
- 공격 유형별 자동 검증 알고리즘을 적용하여 실시간으로 보안관제를 실시함
  - 탐지 패턴을 우회하는 신종 또는 변종 공격 및 탐지 패턴이 없는 공격에도 대응할 수 있음
  - 대용량 사이버 공격을 직관적으로 인지할 수 있음
  - 사이버 해킹공격 탐지 · 자동분석 정확도 향상
  - 보안 이벤트에 대한 빠른 대응이 가능함
  - 분당 1백만 건의 보안이벤트 처리 및 자동분석 유형에 해당되는 사이버 침해위협은 10분 이내 대응 가능함

주요기술 구성 및 구현방법

| 주요기술 구성 |

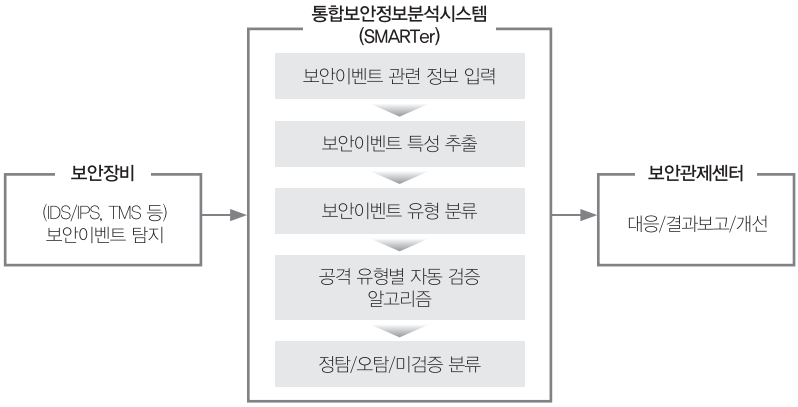
보안이벤트 자동 검증

- 탐지규칙 기반 보안장비에 의해 공격으로 탐지된 보안이벤트 및 보안이벤트와 관련된 정보를 입력함(입력 모듈)
- 입력된 보안이벤트의 특성을 추출함(특성 추출 모듈)
- 시그니처 기반의 보안이벤트인 경우, 공격 유형에 따라 분류함(유형 분류 모듈)
  – 공격 유형 : 악성 URL, 악성코드 다운로드, 정보 전송, 파일 업로드, 악성코드 감염
- 공격유형에 대한 자동 검증 알고리즘에 따라 추출된 보안이벤트의 특성과 입력된 보안이벤트와 관련된 정보를 비교하여 정탐인지 오탐인지 여부를 검증함(자동 검증 모듈)



| 구현방법 |

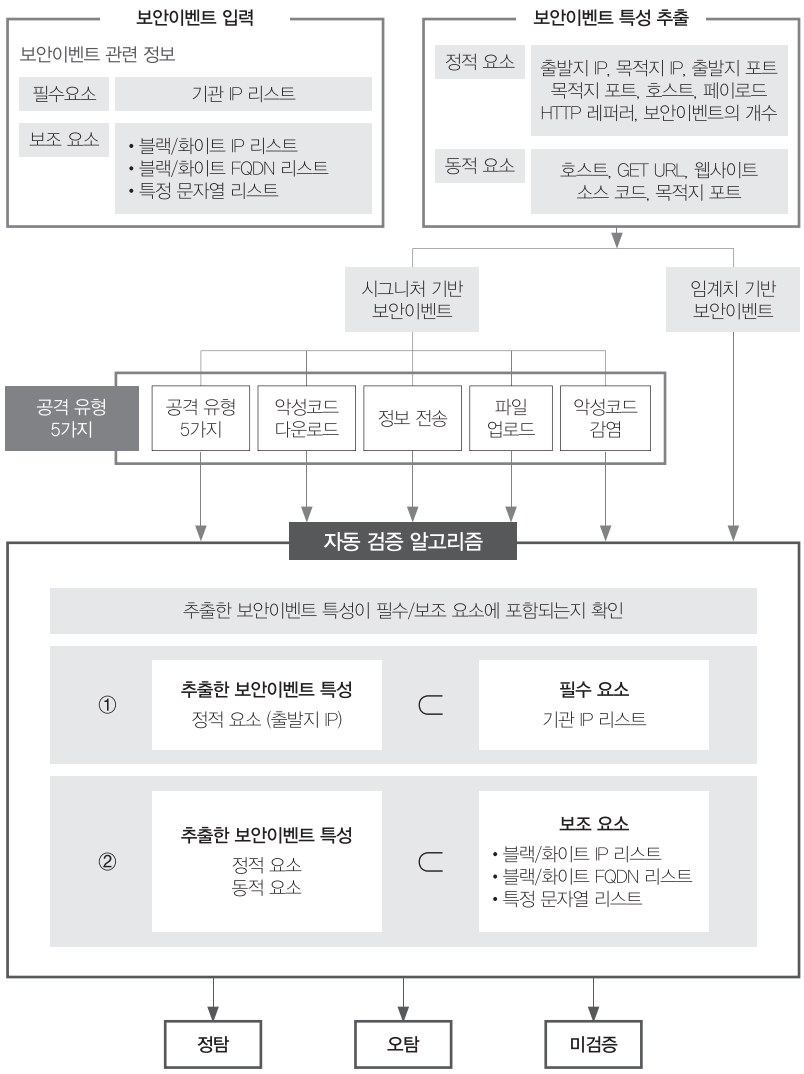
첨단연구망 실시간 보안관제 체계 구축을 위한 통합보안정보분석시스템(SMARTer*)



* "SMARTer" : Security Monitoring, Analysis and Response soluTion extended release

| 구현방법 |

통합보안정보분석시스템(SMARTer)

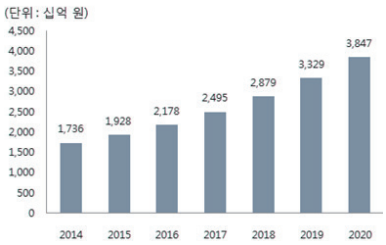


기술/시장 동향

| 기술 동향 |

- 정보보안
  - 사이버 공격에 취약한 자체 구축형(on-premise) 솔루션을 지양하고, 클라우드 기반 통합 보안 방식으로 급속한 전환이 진행 중임
  - 빅데이터를 기반으로 하는 머신 러닝과 인공지능 기술을 활용하여 사이버공격의 유발 환경, 유형, 빈도 등을 분석함으로써 실시간으로 범죄 발생을 예측, 예방하는 솔루션으로 진화하고 있음
- 보안관제
  - 클라우드 · IoT 확대로 공격에 노출되는 지점(Attack Surface)이 늘어나고 있어서 내부 시스템에서 침해 흔적을 찾아 분석해 피해 확산을 막고 유사한 공격을 차단하는 탐지 · 대응 방안이 다양하게 제시되고 있고, 나아가 머신러닝 기술을 적용해 시스템이 스스로 학습하고 정상 상태와 다른 정황을 탐지하면서 고도화되고 있음

기술/시장 동향



[국내 정보보안산업 매출 전망]

※출처 : 중소기업기술로드맵 2016

| 시장 동향 |

- 국내 정보보안시장 규모는 2014년 1조 7.359억 원에서 연평균 14.18%씩 성장하여 2020년에는 3조 8.469억 원 규모로 증가할 것으로 전망됨
  - 2020년까지 제품 부문은 연평균 15.2% 증가하여 3조 178억 원, 서비스 부문은 13.6% 성장하여 8.290억 원에 달할 것으로 예상됨
- 2015년 기준, 국내 보안관제시장은 약 1.937억 원으로 조사됨
  - 국내 파견관제 시장은 2015년 기준 약 1,000억 원의 시장규모이며 2020년까지 약 2,000억 원대로 성장할 것으로 예상됨
- 세계 정보보안시장은 2021년 약 1.200억 달러 규모로 전망됨
  - 2015~ 2021년 연평균 8.1%의 성장률

활용분야 및 권리현황

| 기술활용분야 |

기술 수요처	적용처
연구기관	보안관제/긴급대응 지원
사이버안전센터	보안관제시스템
기업체	실시간 보안관제 서비스

| 권리현황 |

- 국내 등록특허 5건, 출원특허 1건, 해외 출원특허 1건

발명의 명칭	특허번호	비고
보안이벤트 자동 검증 방법 및 장치(악성 URL 공격 유형)	10-1689295	등록
보안이벤트 자동 검증 방법 및 장치 (악성코드 다운로드 공격 유형)	10-1689296	등록
보안이벤트 자동 검증 방법 및 장치 (정보 전송 공격 유형)	10-1689297	등록
보안이벤트 자동 검증 방법 및 장치 (파일 업로드 공격 유형)	10-1689298	등록
보안이벤트 자동 검증 방법 및 장치(임계치 공격 유형)	10-1689299	등록
보안이벤트 자동 검증 방법 및 장치 (악성코드 감염 공격 유형)	10-1890272	등록
METHOD AND DEVICE FOR AUTOMATICALLY VERIFYING SECURITY EVENT	PCT-KR2016 -001512	해외 출원

추가기술정보

기술분류 슈퍼컴퓨터 – 첨단 연구망

시장전망 전세계 정보보안 시장은 연평균 8.1% 의 성장률로 지속적 성장이 전망됨

기술문의 최장원 책임연구원 (국가슈퍼컴퓨팅본부) 042-869-1058 | jwchoi@kisti.re.kr
윤신혜 행정원 (성과확산실 기술이전 담당) 042-869-1832 | shyoon@kisti.re.kr