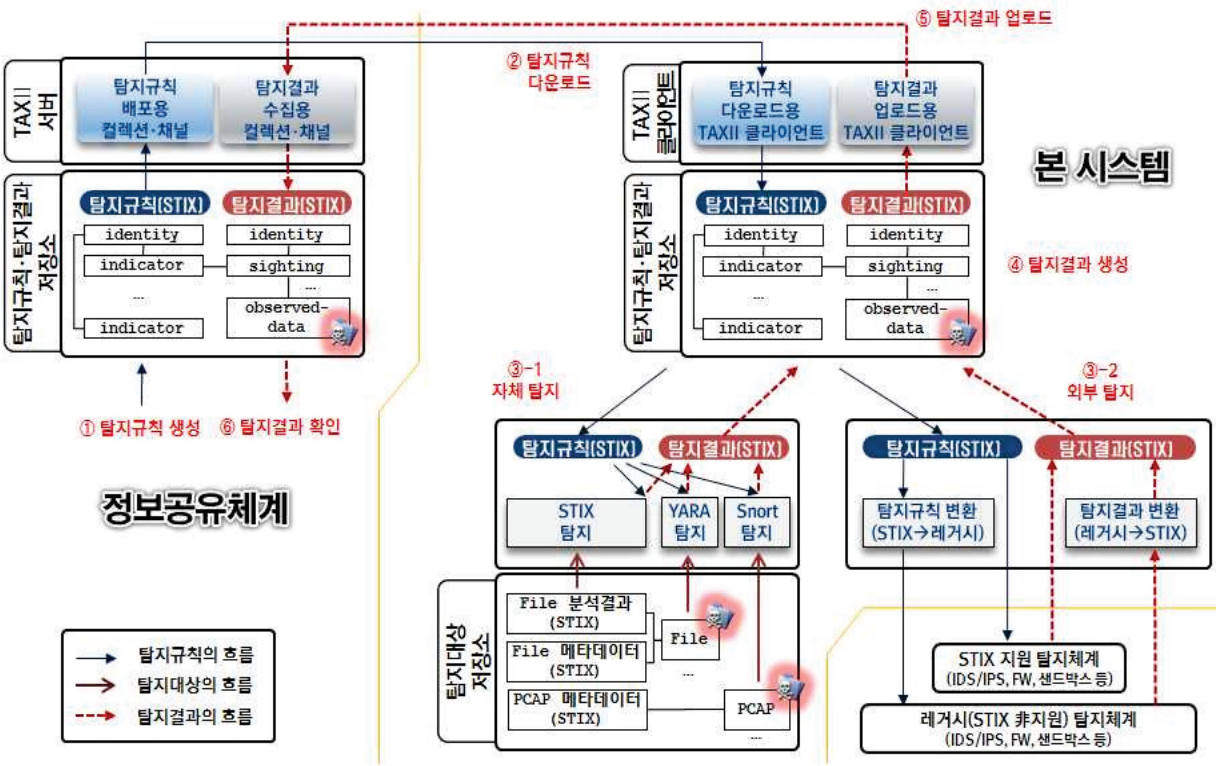
STIX 및 TAXII 기반 악성파일 탐지기술

기술키워드	악성파일, 악성코드, 표준, 탐지, STIX, TAXII, CTI, YARA, Snort								
지식재산권	등록 2건(대한민국) TTA 국내표준 1건								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	**시제품 제작**	시제품 성능평가	시제품 신뢰성평가	시제품 인증	상용품

기술개요

- 세부기술[1] - **최신 CTI 기술규격을 기반으로 악성파일 및 악성행위에 대한 탐지 및 탐지결과 수집 자동화**
  · 계층구조를 가지는 여러 기관에서 악성파일과 악성행위를 자동화된 방법으로 탐지하고 결과를 수집
  · STIX 2.0(이상) 및 TAXII 2.0(이상)을 100% 준수(STIX Patterning Conformance Level 2 만족)
- 세부기술[2] - **탐지규칙, 탐지대상, 탐지결과 등 STIX 객체 간 관계인식 및 관리**
  · STIX 객체들간의 관계를 효과적으로 관리하고 인식
  · 실제객체(예: 파일 등)와 이에 대한 STIX 객체간 관계인식 및 관리
- 세부기술[3] - **악성코드 행위 정규화, 시각화 및 고속 필터링**
  · 행위 및 객체를 정규화하고 이를 시각적으로 표현하며, 탐지성능 향상을 위한 고속 필터링
- 기술 구성도



(그림 5-1) 시스템 구조

기술성

- 최신 CTI 기술규격을 기반으로 악성파일 및 악성행위에 대한 탐지 및 탐지결과 수집 자동화
  - 여러 기관에서 악성파일(행위)을 자동 탐지 및 탐지결과 자동 수집
  - STIX, YARA, Snort 탐지패턴 지원(STIX Patterning Conformance Level 2 만족)
  - STIX 2.0(이상) 및 TAXII 2.0(이상)을 100% 준수하는 시스템으로 해당 기술규격을 기반으로 구현되는 타 시스템과의 연동을 보장
  - 파일 및 PCAP 메타데이터 처리를 통한 탐지 고속화
- 탐지규칙, 탐지대상, 탐지결과 등 STIX 객체 간 관계인식 및 관리
  - STIX 객체들간의 관계를 효과적으로 인식하고 관리
  - 실제객체(예: 파일 등)와 이에 대한 STIX 객체간 관계인식 및 관리
- 악성코드 행위 정규화, 시각화 및 고속 필터링
  - 악성코드의 행위와 관련객체를 정규화(index 기반)된 방법으로 인식하고 시각적으로 표현
  - 악성코드에 의해 발생한 행위와 객체 정보를 토대로 메타데이터를 구성하여 필터링(탐지속도 향상)

시장성

- 일원화된 악성코드 탐지체계 구축 시 기반기술로 활용
  - TTA 표준(표준명: STIX 기반 사이버위협 정보공유 체계와 레거시 탐지체계의 연동을 위한 시스템 구조, '18.6. 제정예정)의 최소한의 요구사항을 만족하는 본 기술을 도입하여 후발 보안업체의 시장 진입 장벽 낮춤
- 최신 CTI 기술규격의 국내 도입 활성화를 통해 글로벌 경쟁력 향상
  - STIX 및 TAXII 보안규격을 기반으로 하는 CTI 체계의 구축이 사이버위협 탐지·대응 분야에서 주력 기술로 평가받고 있음
  - 따라서, 국내 보안업체들이 최신 규격인 STIX 2.0(이상) 및 TAXII 2.0(이상)을 기반으로 하는 본 기술을 적용하여 보안제품을 개발하면 국내 보안업계의 글로벌 경쟁력 향상

기술 응용 분야

- 일원화된 악성코드 탐지체계 구축
- 국내 보안시장을 글로벌 표준인 STIX, TAXII 기반으로 재편하여 국내 보안업계의 국제 경쟁력 향상

기술개발 완료시기

- 2018년 4월 완료

관련 특허 등 지식재산권

- (등록) 10-1818006(2018. 1. 8. 대한민국) "행위 정규화를 통한 악성코드 고속탐지 및 시각화 방법 및 이를 이용한 장치"
- (등록) 10-1964592(2019. 3. 27. 대한민국) "보안위협 정보 공유 장치 및 방법"
- (TTA 국내표준) TTAK.KO-12.0326(2018. 6. 27.) "STIX 기반 사이버위협 정보공유 체계와 레거시 탐지체계의 연동을 위한 시스템 구조"