10 초연결네트워크

보안 관제 : 보안위협 정보 공유 기술

- 특허명 : 보안위협 정보 공유 장치 및 방법(10-2018-0048084)
- 보유기관 : 국가보안기술연구소
- 상태정보 : 출원 '18.04.25 등록 '19.03.27
- 기타정보 : 관련특허 포트폴리오 구축(총 2건)

특허원문보기

기술개요

· 최신 CTI 기술규격을 기반으로 악성파일 및 악성행위에 대한 탐지 및 탐지결과 수집 자동화
· 탐지규칙, 탐지대상, 탐지결과 등 STIX 객체 간 관계인식 및 관리
· 악성코드 행위 정규화, 시각화 및 고속 필터링
· 보안 관제 서비스, 보안 관제 장비, 네트워크 보안 산업 등

기존 문제점

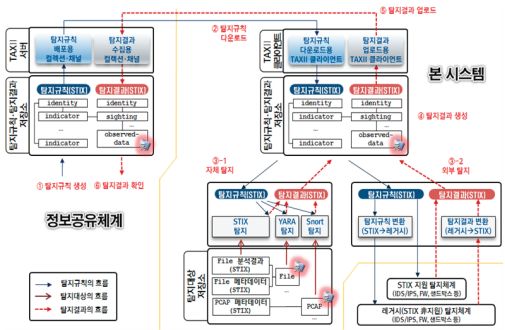
· 벤더별로 추출 가능한 정보가 상이하며, 타사 장비와 연동되지 않음
· 보안 관제 장비가 벤더 자체 탐지 규칙을 사용한 경우 타사 장비로 이전 어려움
· 특정 벤더의 보안 장비에 의존적

기술 차별점

· 보안위협 정보를 체계화하여 이종 벤더 간 공유
· 벤더별로 상이한 정보 및 정보의 전송 방식을 규격화 하여, 이종 벤더 간 정보 공유 체계의 연동성을 확보

세부내용

· 제공계층구조를 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)
· 실제객체(예: 파일 등)와 이에 대한 STIX 객체간 관계인식 및 관리
· 행위 및 객체를 정규화하고 이를 시각적으로 표현하며, 탐지성능 향상을 위한 고속 필터링



기술이전 문의
· 국가보안기술연구소 주익수(042-870-4965, tech@nsr.re.kr)
· 공동마케팅사무국 이가영(042-862-6985, gylee@wips.co.kr)