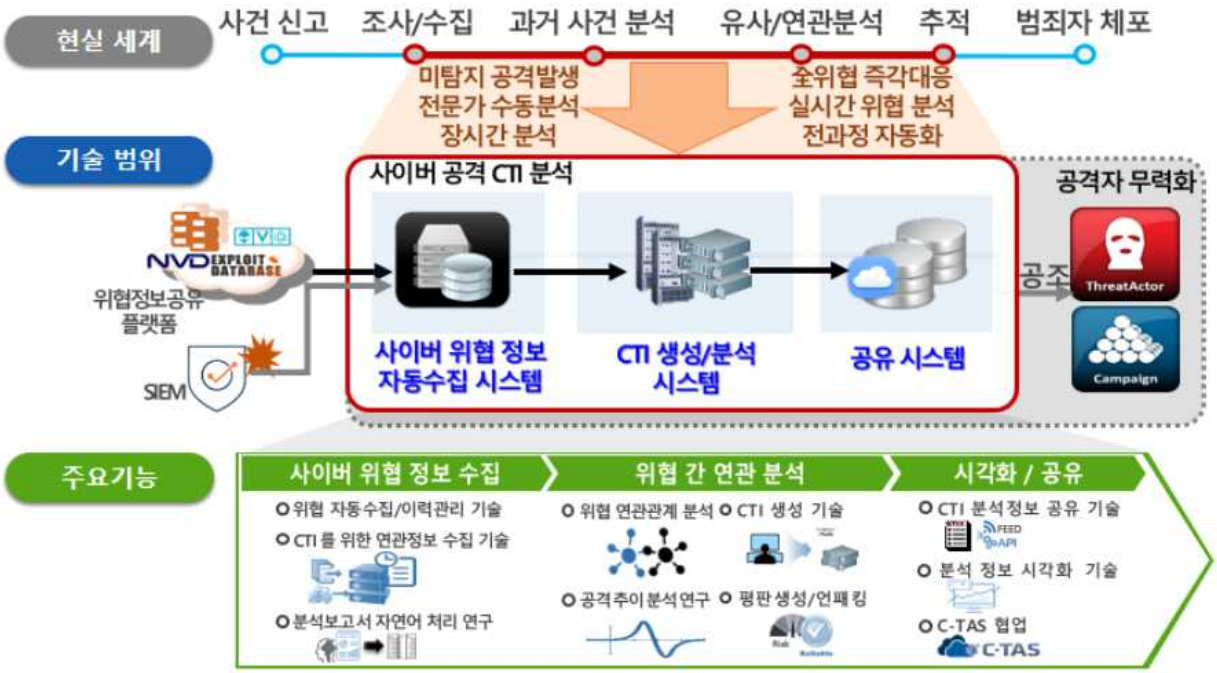
Ⅱ. 20년 기술이전 대상 목록

④ 국가 차원의 침해사고 대응을 위한 사이버 위협 인텔리전스 분석(CTI) 및 정보 공유 기술 ('17.3월 ~ '19.12월(3년))

□ 기술개요

o 지속적으로 발생하고 있는 **유사/변종 사이버 위협**에 능동적인 대응이 가능한 침해정보 과거이력 수집 및 **실시간 위협 인텔리전스 분석을 통한 사이버 위협 정보 공유 기술 개발**

< 기술 개념도 >



□ 기술의 특징 및 장점

o OSINT 기반 침해공격 이력 정보 종합관리
- 공격 시점의 침해공격 이력 정보 부족으로 인한 분석 장기화 방지
- 단편적 OSINT 정보 복합 분석을 통한 실행가능한 분석데이터 자동 생성

o 공격 그룹 프로파일링을 통한 위협 분석 초기에 사이버 위협 정보 간 상호 연관성 파악

o 위협 인텔리전스 공유를 통한 능동적인 사이버 공격 대응

□ 활용 분야

① 사이버 위협정보 수집/이력관리 (보안관제, 침해사고 분석, 네트워크 보안분석)

② 사고 단계별 유사/변종 사이버 공격 분석 및 차단(침해사고 분석, 네트워크 보안분석)

□ 기술이전 내용 및 범위

구분	시스템	주요 내용
1	CTI 수집 시스템	o 가상화 기반 악성코드 수집, 악성코드 위협 정보 및 부가정보 자동 수집 기술 o 악성 IP, Domain 정보 및 연관된 정보 자동 수집, 취약점 정보 수집/저장/관리 기술
2	CTI 분석 시스템	o 그래프 기반의 공격 연관관계 분석 및 위협정보 그룹 클러스터링 기술 o 사이버 위협정보 그룹 내 핵심 위협요소 분석 및 악용자원 추정 기술 o 세부 기술 구성 - 기술1 : 공격 분석을 위한 연관 위협 정보 수집/관리 모듈 - 기술2 : 그래프 분석 기반의 공격 연관 분석 및 위협 탐지 모듈

□ 세부문의

담당자	김경한 주임연구원(061-820-1307, rndts@kisa.or.kr)