
NCNP

M A S K

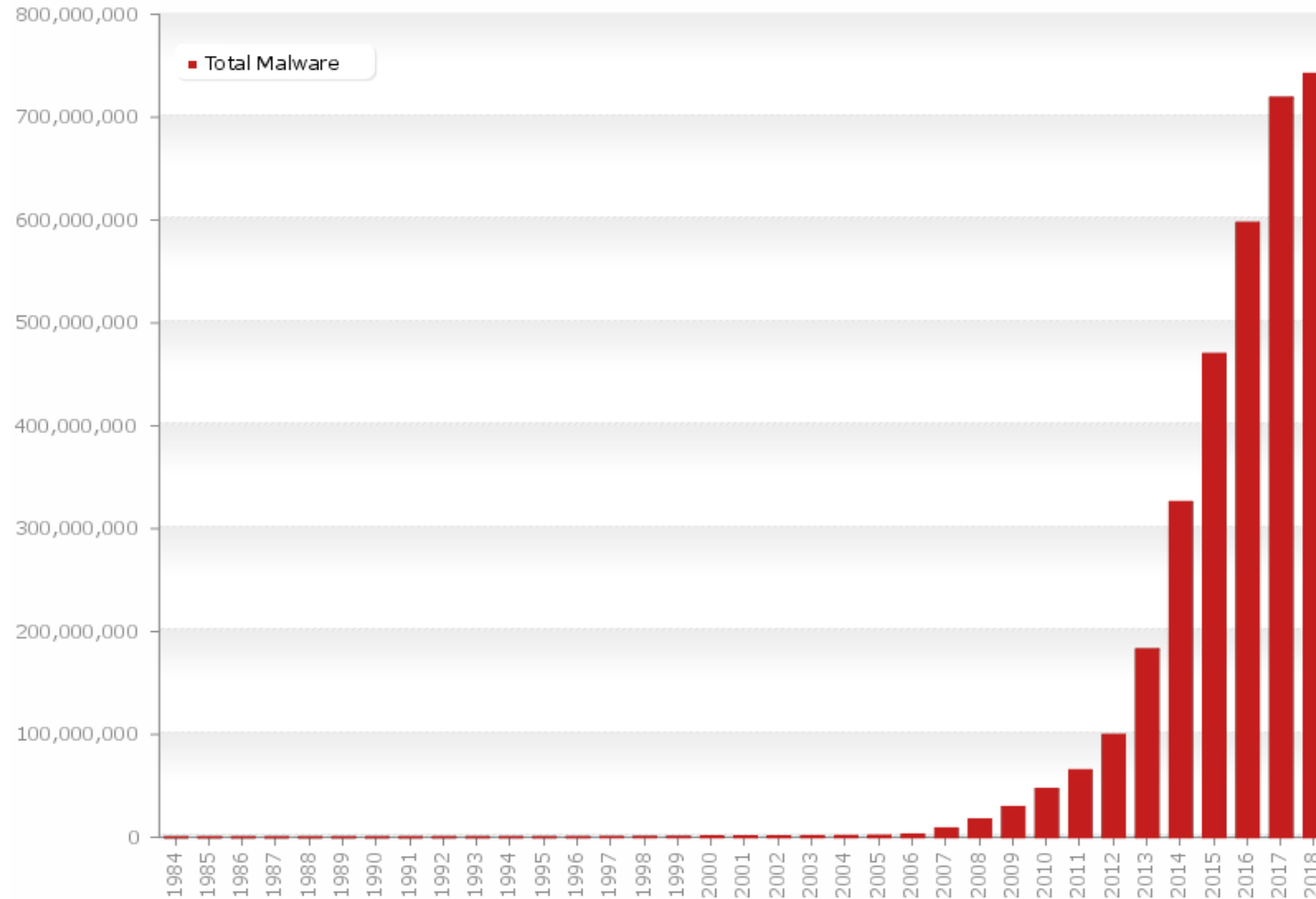
한채연 김영재 명준우 이유정 허준녕

No Commit, No Pay



01 프로젝트 개요

“ 기하급수적으로 증가하는 악성코드 ”



[출처 : AV-TEST]



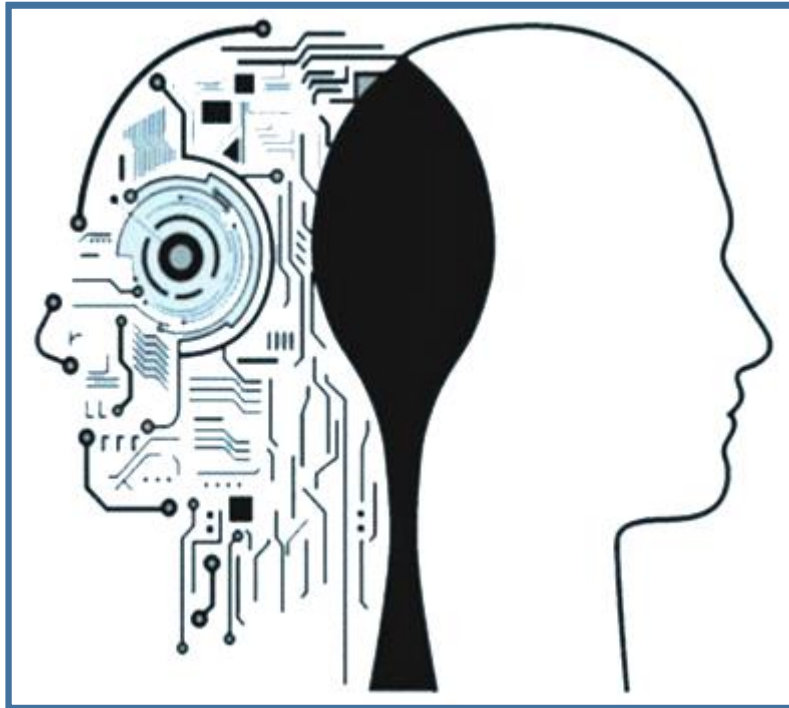
01 프로젝트 개요

“ 그에 비해 현격히 부족한 악성코드 전문가의 수 ”



01 프로젝트 개요

“4차 산업혁명”



01 프로젝트 개요



Malware

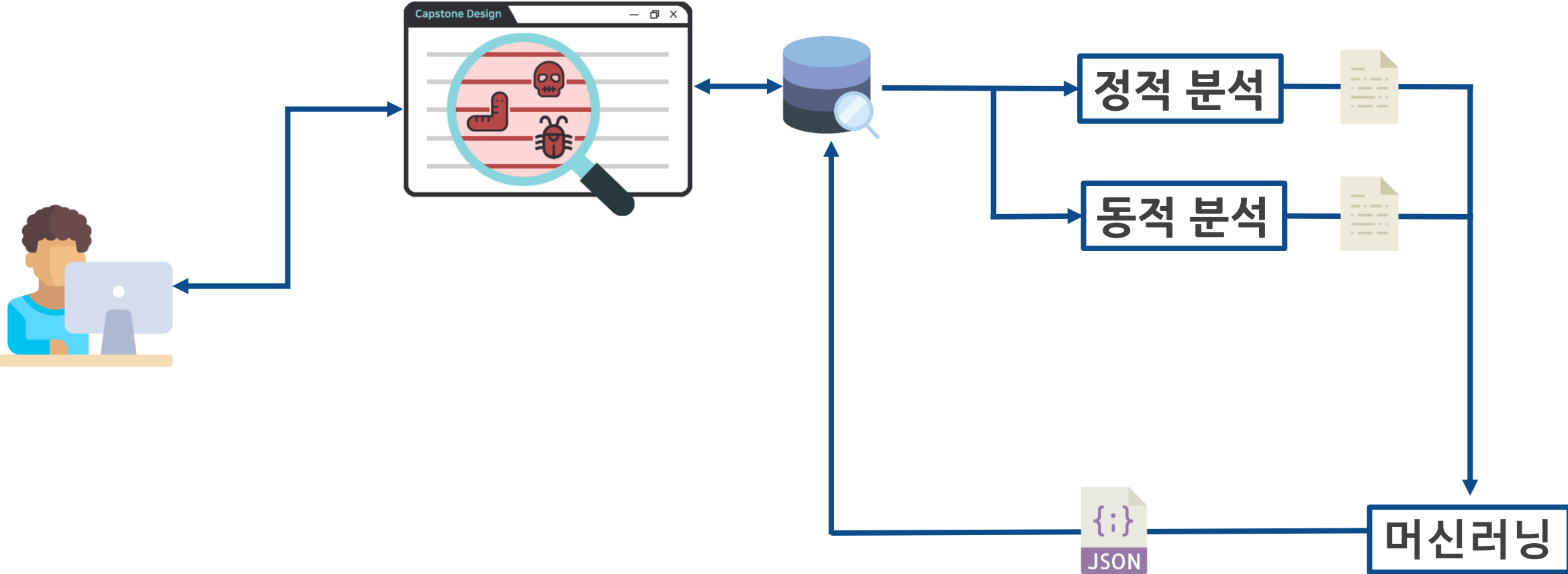
Analysis

System

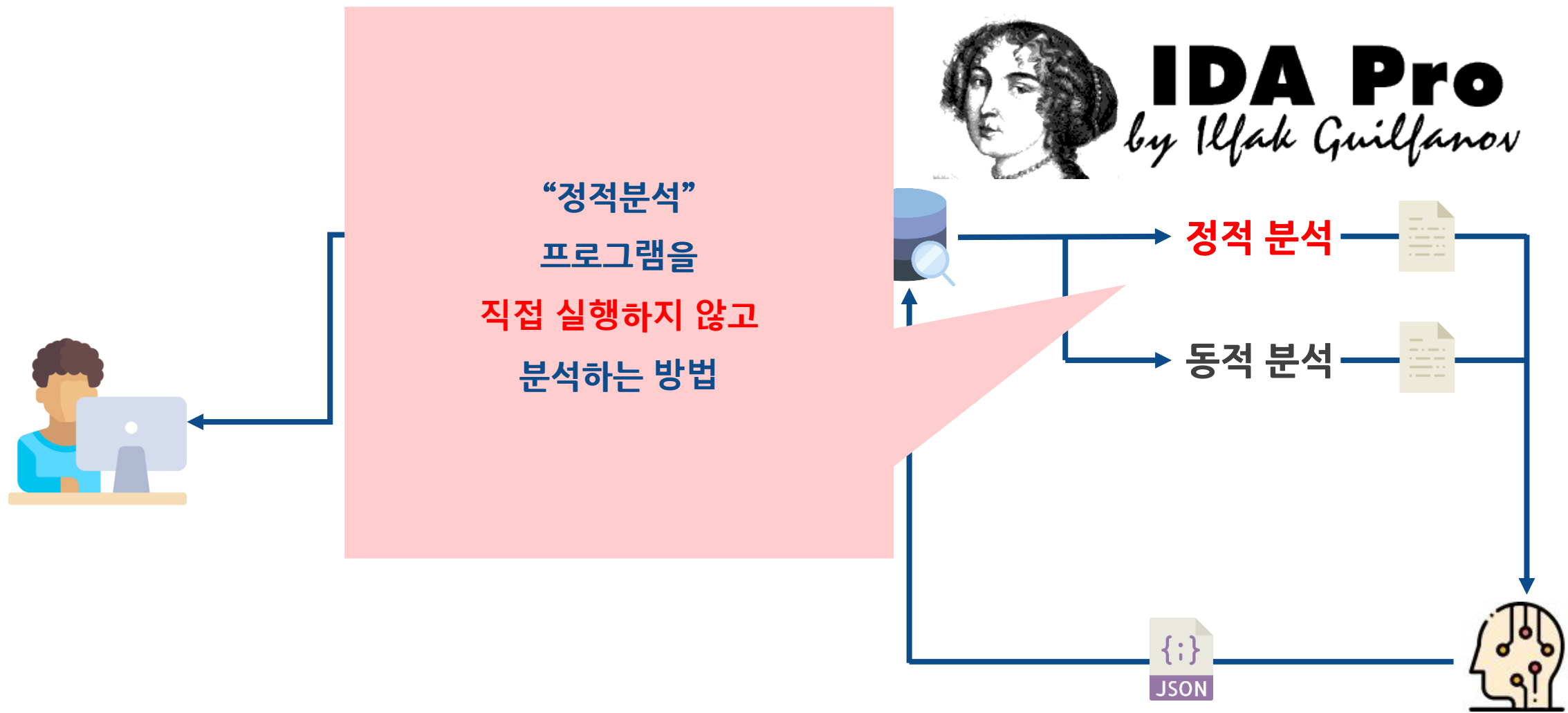
in **K**ookmin



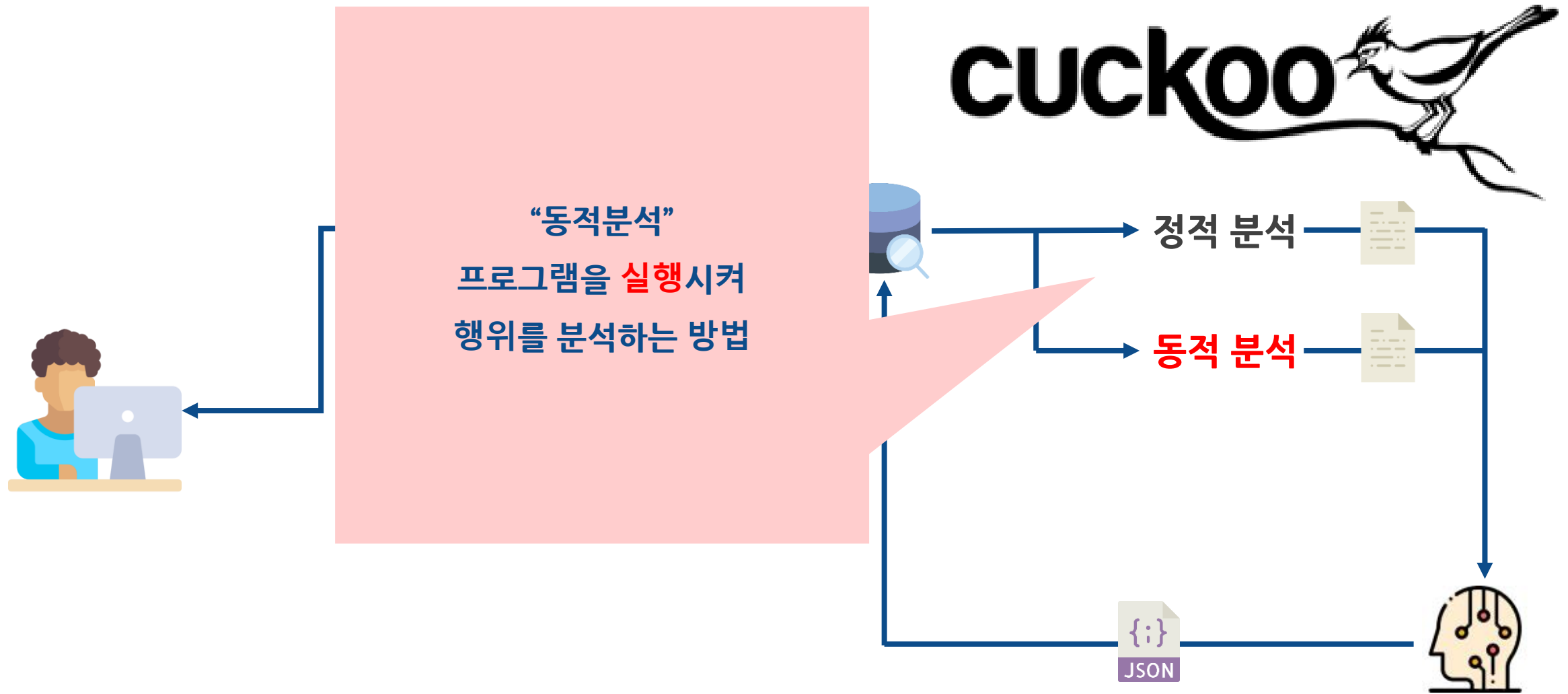
02 목표



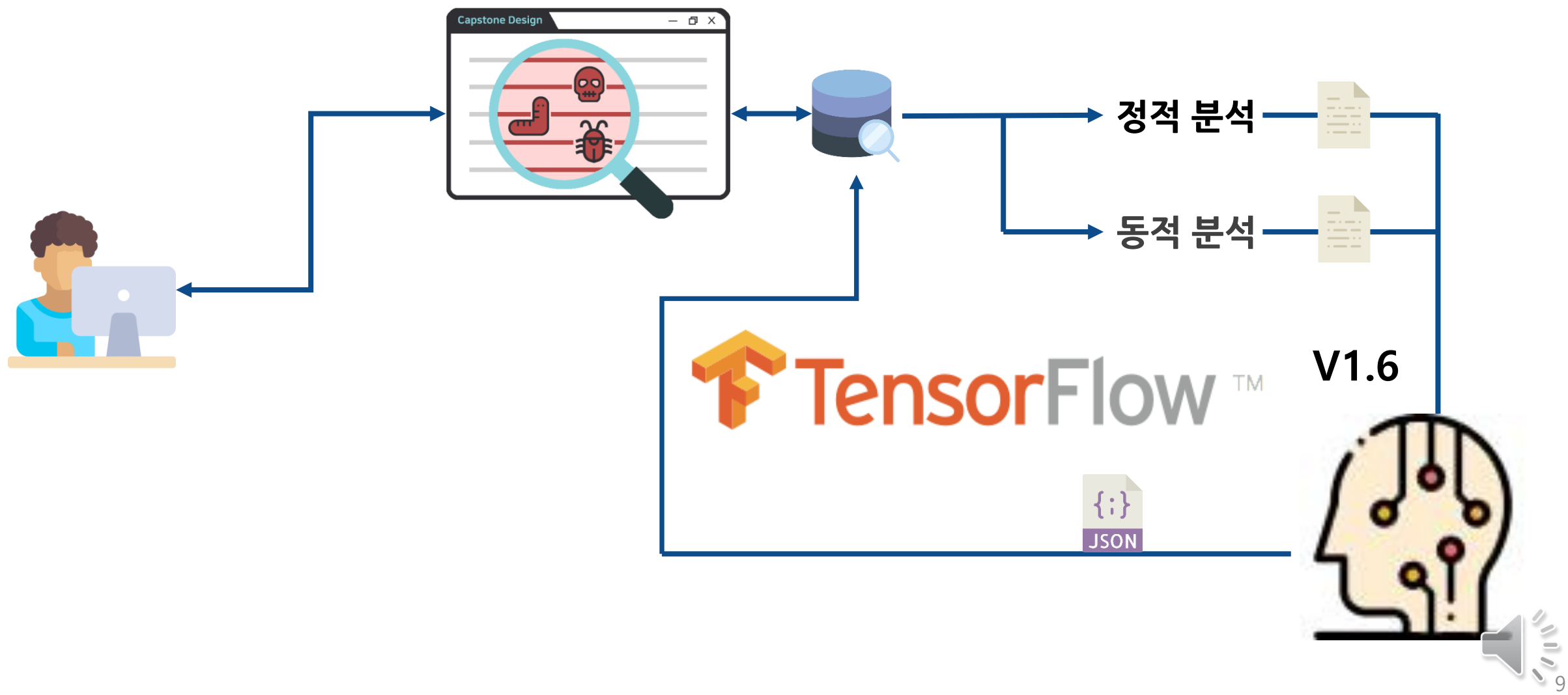
02 목표



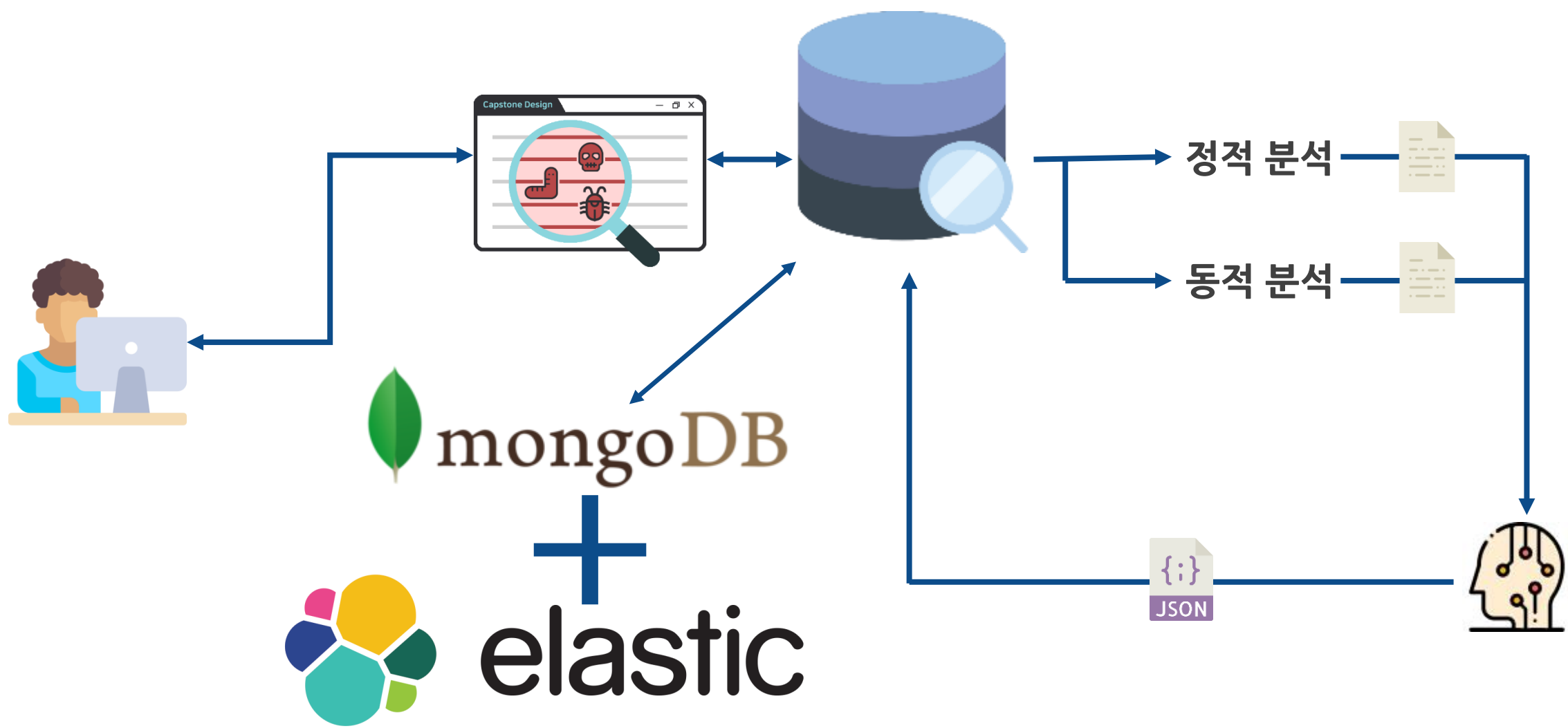
02 목표



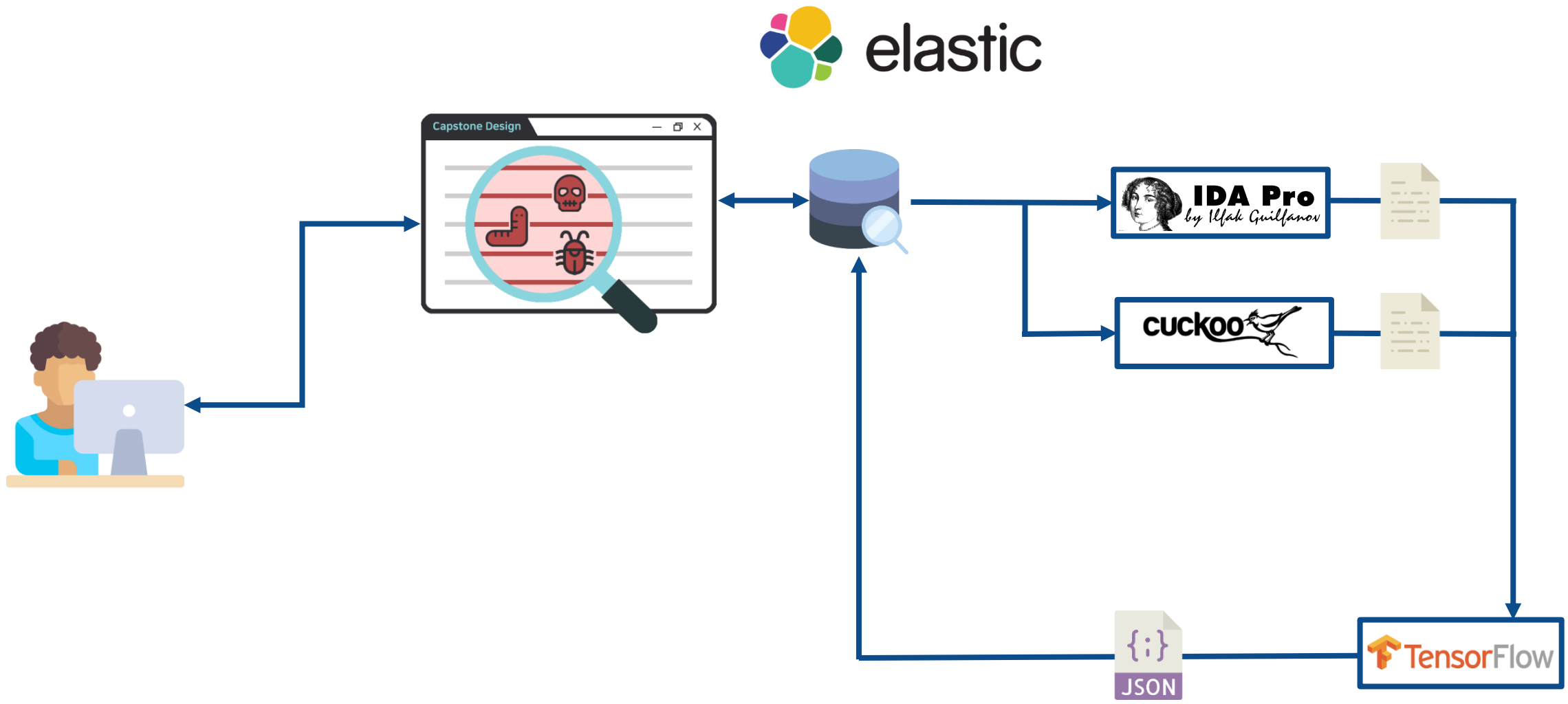
02 목표



02 목표



02 목표



03 기대효과

차별화

- 1 **오픈소스 소프트웨어 제공**
기업에서 상용화 가능



- 2 **유사도 검사**
elastic search



- 3 **많은 양의 학습 데이터**
600만개 이상



04 역할 분담

한채연

- Software Project Leader, 문서작업
- 동적 분석 시스템 최적화, 자동화
- Report로부터 유용한 피쳐들 추출
- 논문 분석 및 연구

김영재

- 정적 분석 시스템 최적화 및 자동화
- 정적 및 동적 피쳐 가공
- 딥러닝 모델 설계 및 구축
- 악성코드 크롤러 제작

명준우

- VirusTotal 분석 리포트 수집
- 동적, 정적 분석 정보를 이용하여 파일 간 유사도 추출
- 악성코드 라벨링

이유정

- 웹 프론트엔드 제작
- 포스터 등 디자인

허준녕

- 프로젝트 인프라 관리
- 데이터베이스 설계 및 SQL 작성, 관리, 검색엔진 구축
- ssdeep을 이용한 파일 유사도 분석
- 웹서버 구축 및 관리

감사합니다
