2020 Capstone Design

SEMO : Security Monitoring Platform

2 차 중 간 발 표

CONTENTS

SEMO : Security Monitoring Platform

CONTENTS

SEMO : Security Monitoring Platform

01 프로젝트 소개

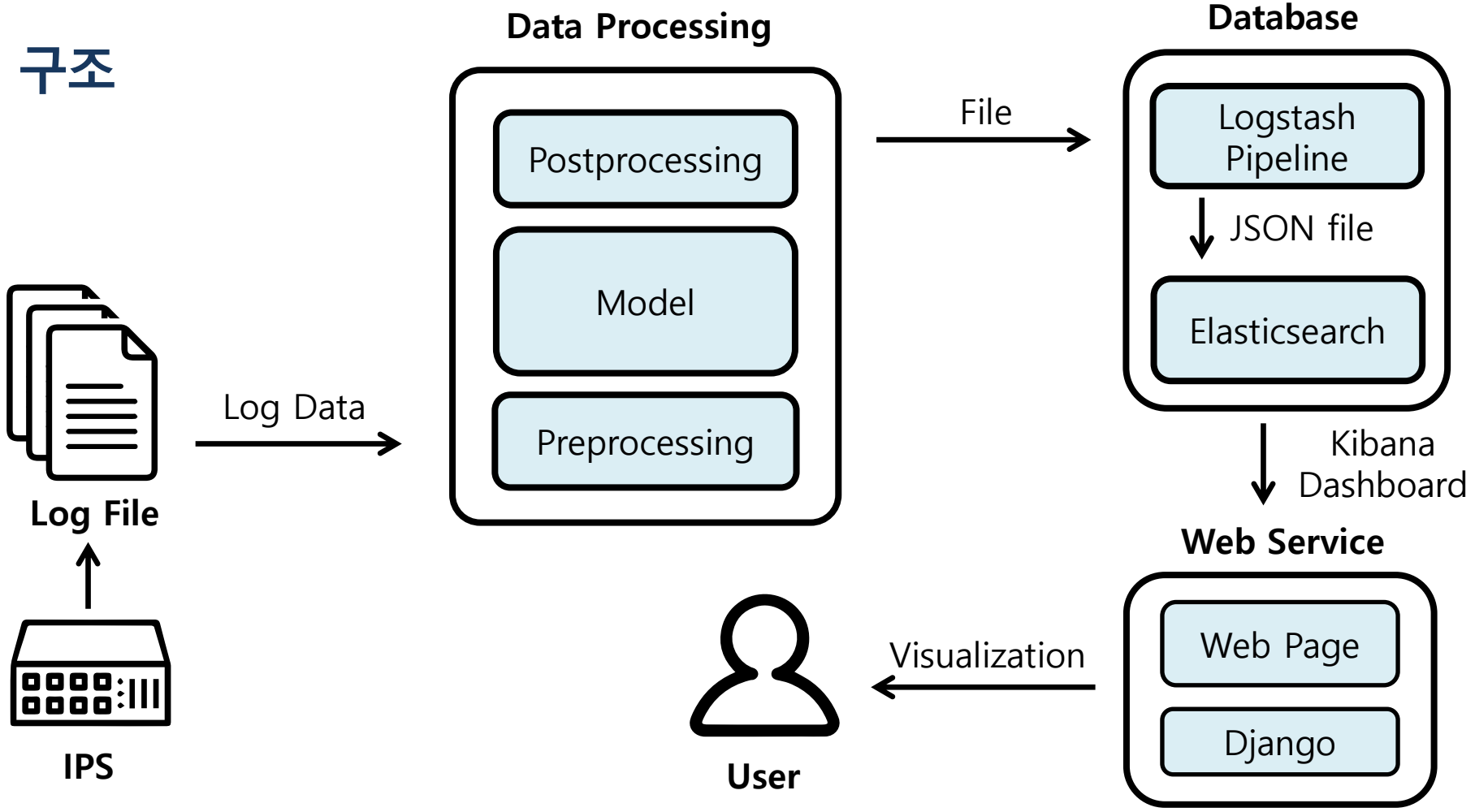
프로젝트 소개

“ 증가하는 데이터, 방대한 트래픽 양 ”

“ 보안 업무 효율성 향상 ”

01 프로젝트 소개

시스템 구조

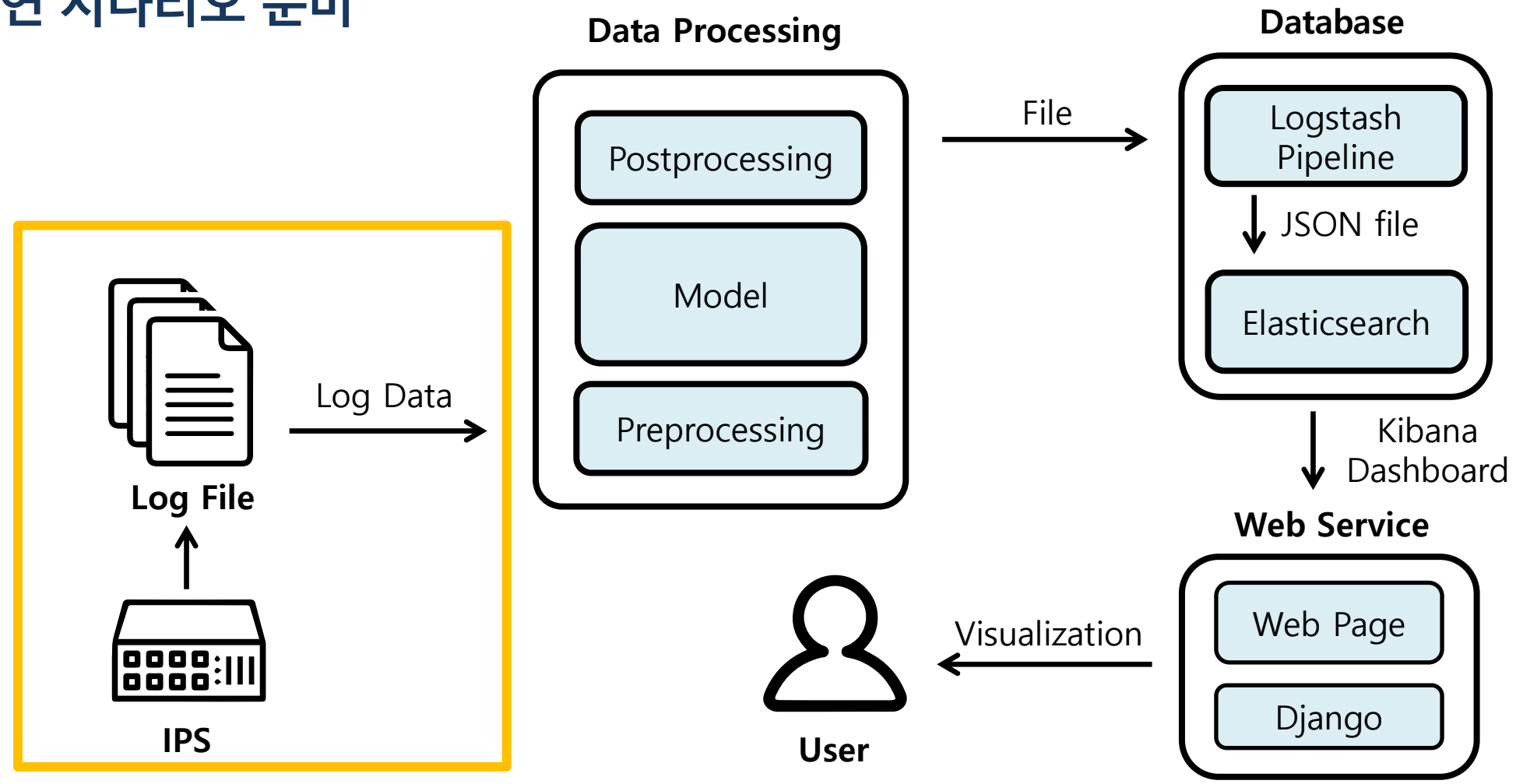


CONTENTS

SEMO : Security Monitoring Platform

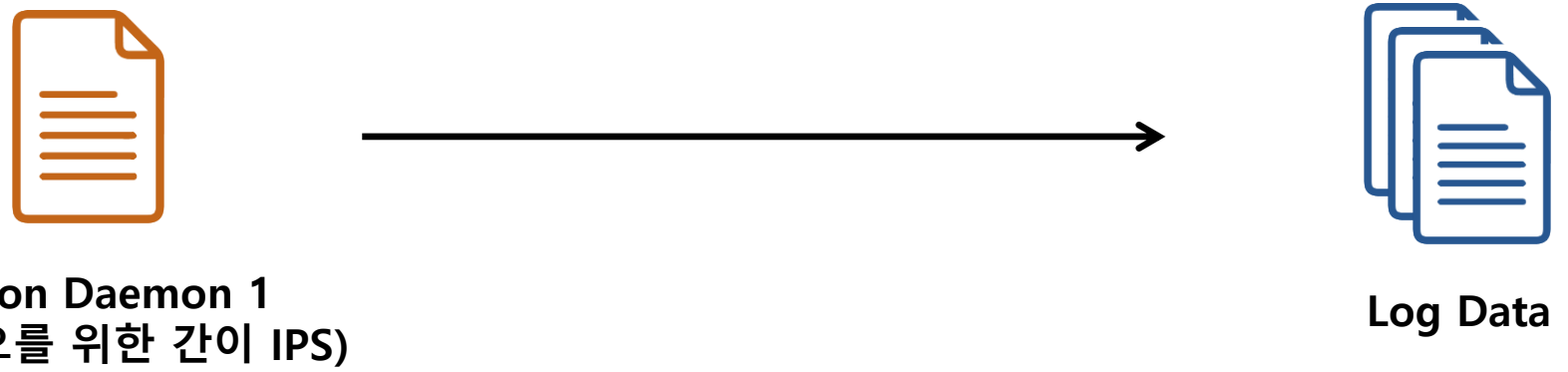
02 수행 내용

시연 시나리오 준비



02 수행 내용

시연 시나리오 준비

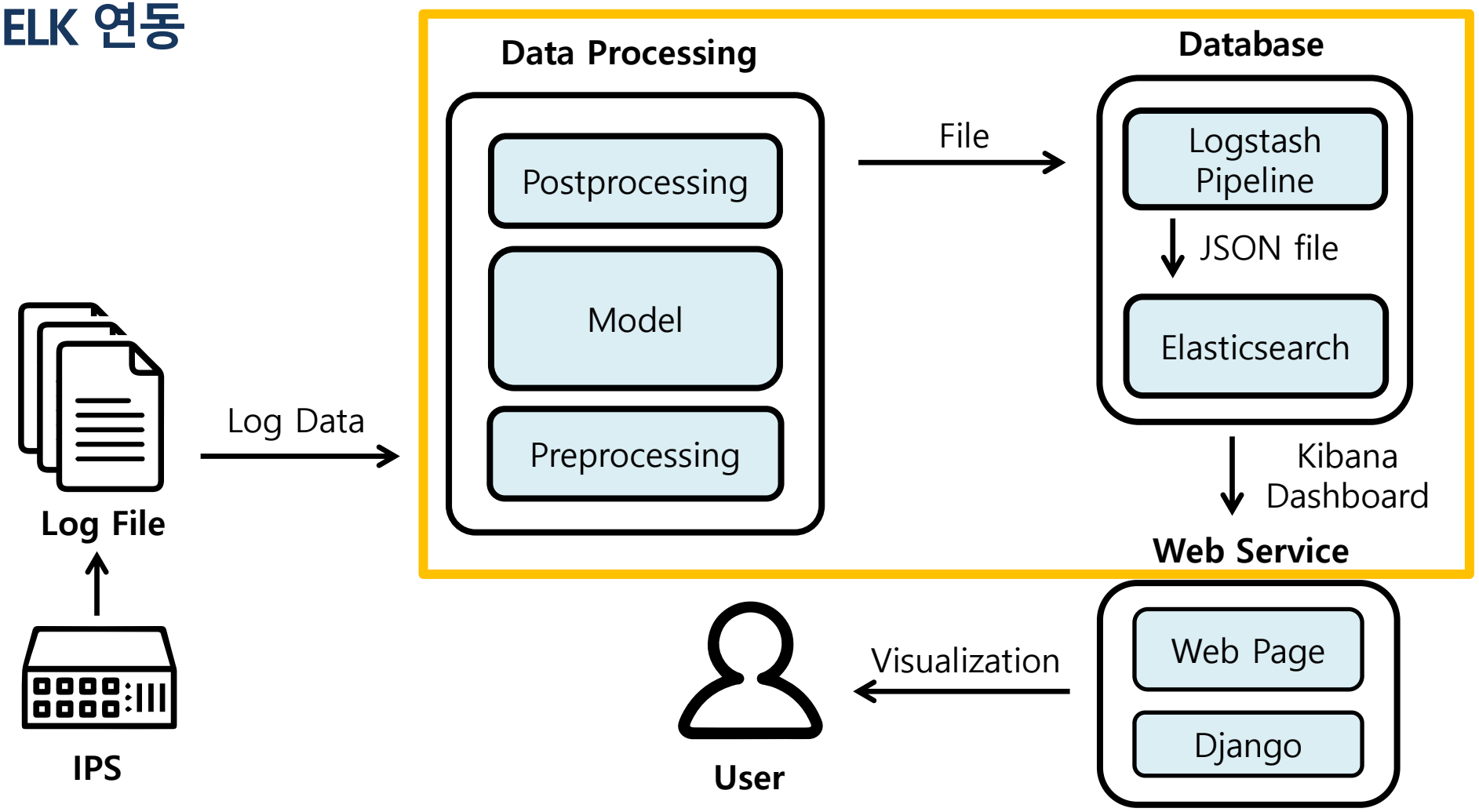


02 수행 내용

시연 시나리오 준비

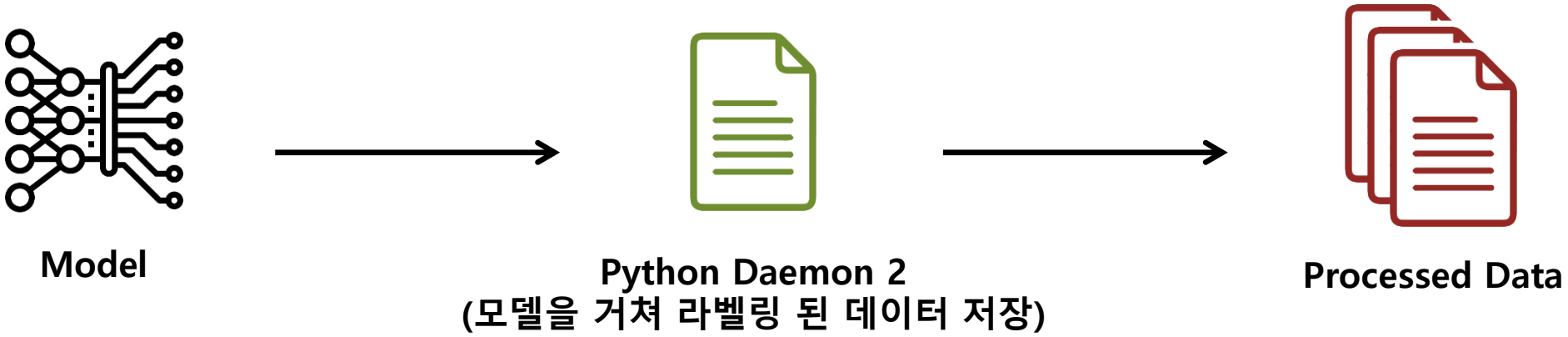
02 수행 내용

모델 - ELK 연동



02 수행 내용

모델 – ELK 연동

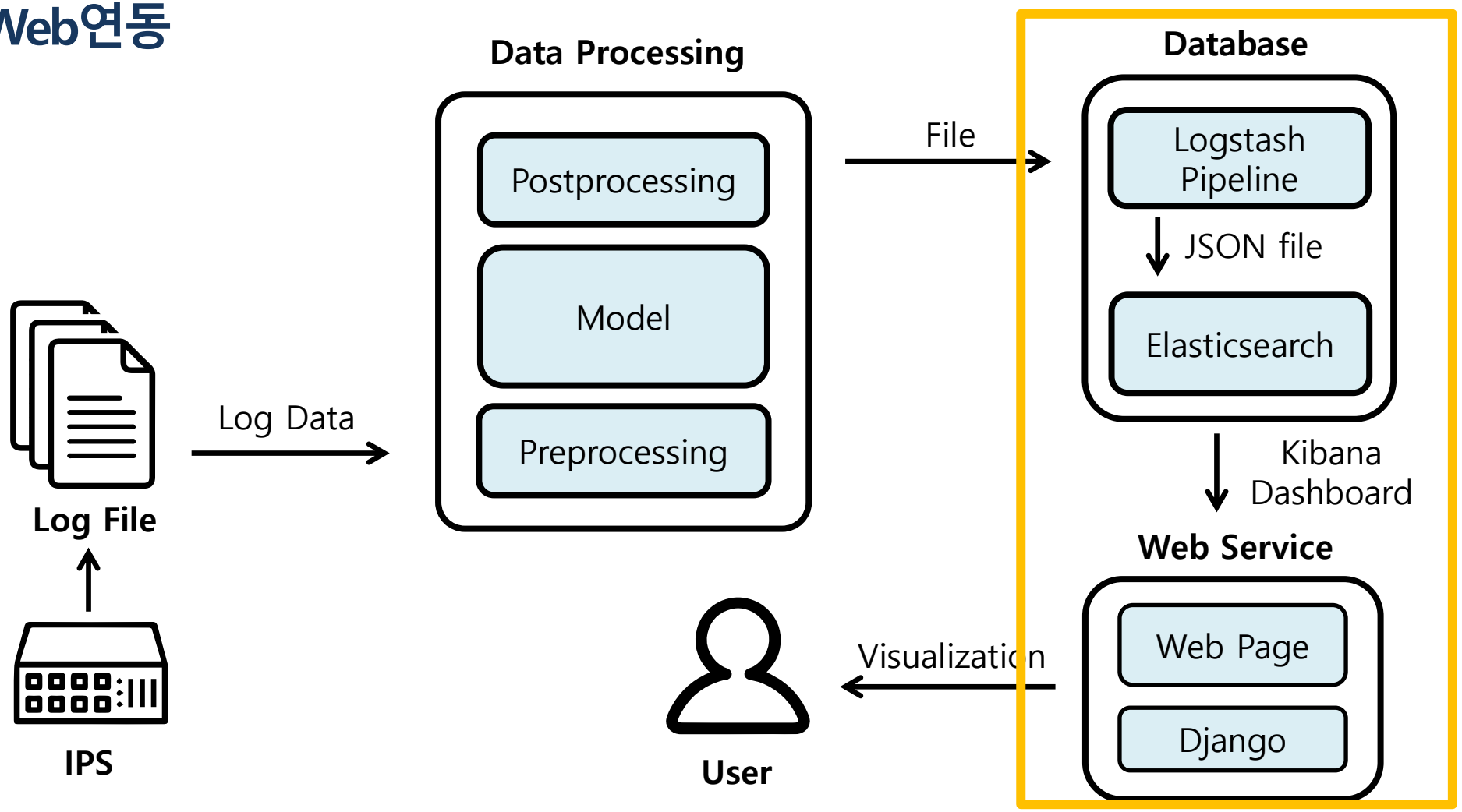


02 수행 내용

모델 – ELK 연동

02 수행 내용

ELK – Web연동

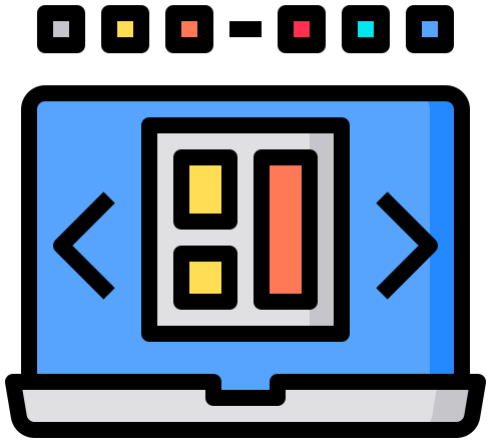


02 수행 내용

ELK – Web연동

Kibana 대시보드

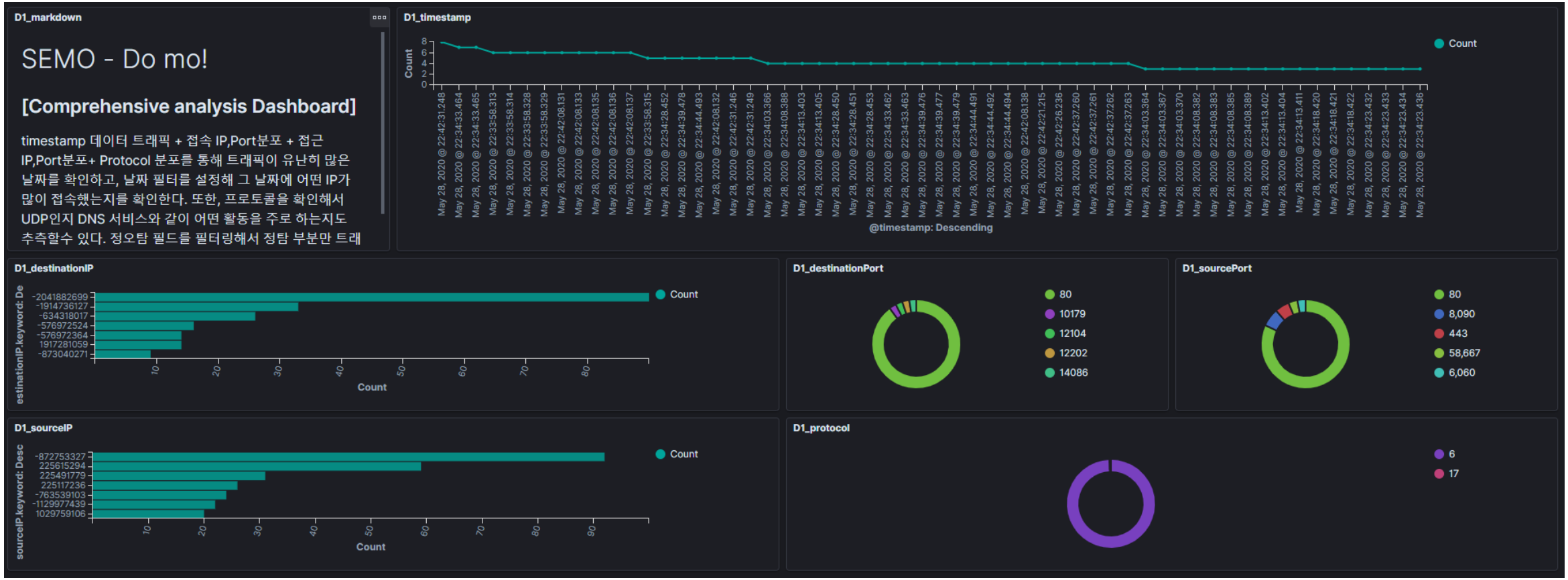
Embed code(URL)



Django templates

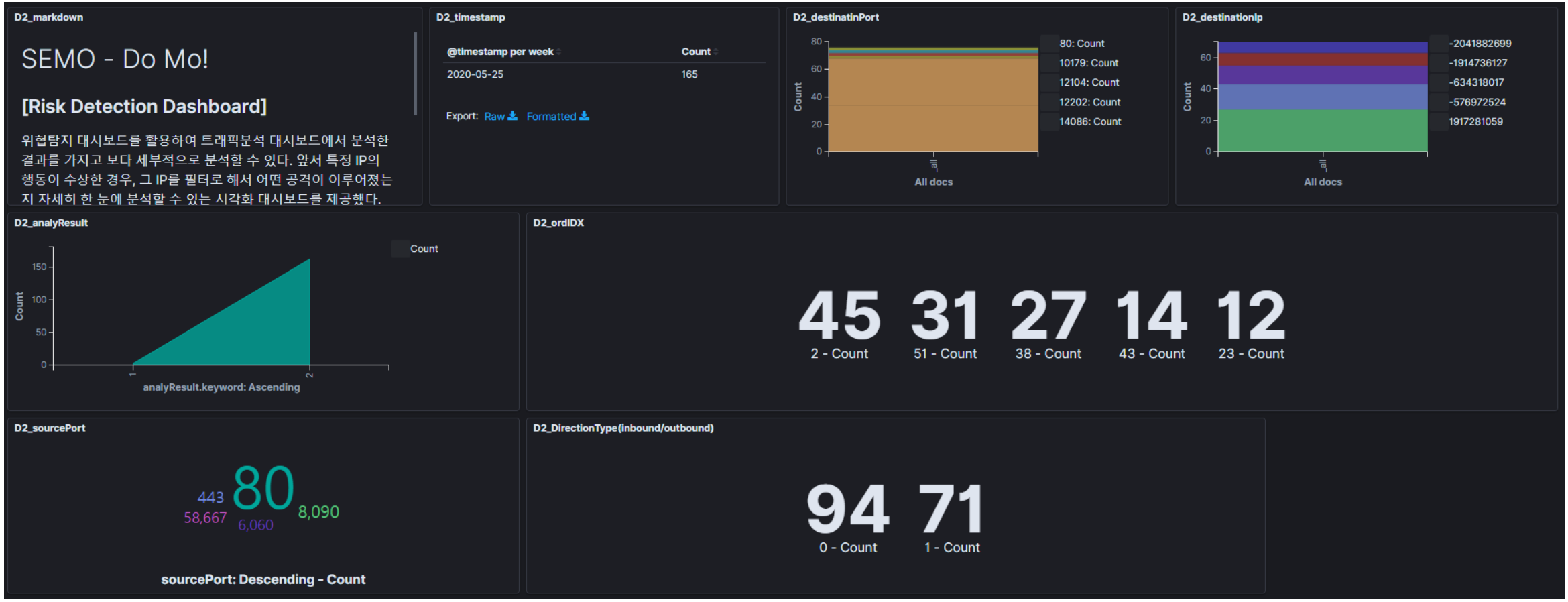
02 수행 내용

대시보드 구성



02 수행 내용

대시보드 구성



02 수행 내용

ELK 가이드라인 작성

ELK

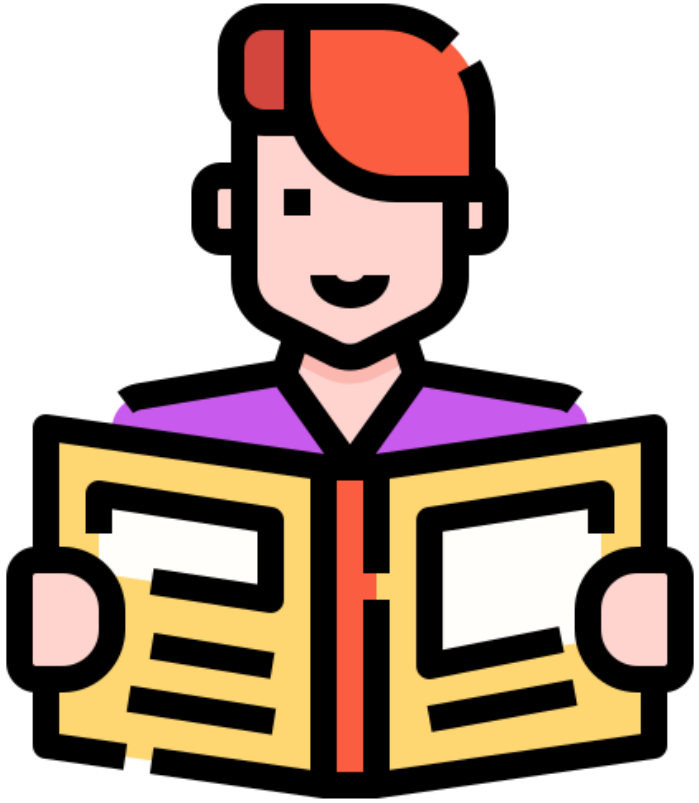
해당 가이드라인은 ELK 스택 7.7 버전을 사용하였으며, 설치 및 사용에 관

설치 순서

ELK Stack 설치 순서는 다음과 같습니다.

1. Elasticsearch
2. Kibana
3. Logstash (여기까지만 설치하시면 됩니다. 아래는 추가적으로 필요한
4. Beats
5. APM Server
6. Elasticsearch Hadoop

이 순서대로 설치하면 각 제품이 의존하는 구성 요소가 제 위치에 있게 됩

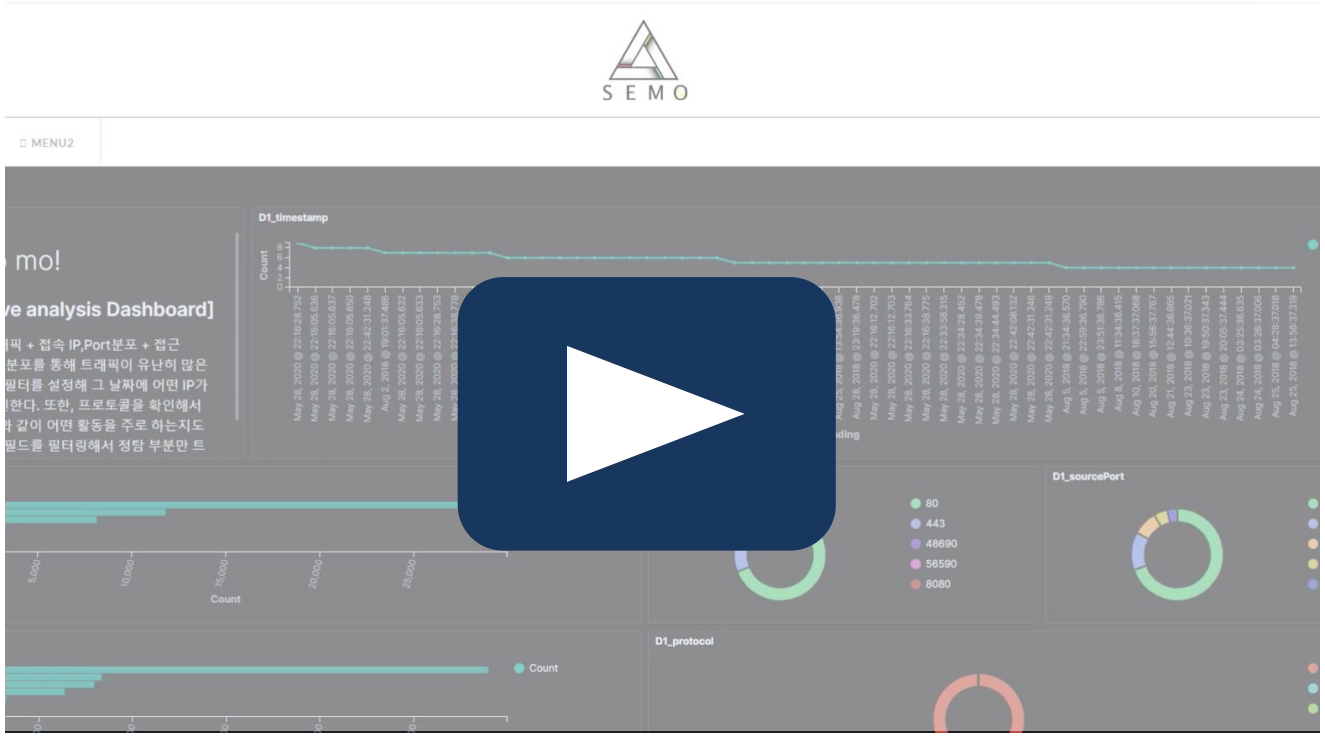


CONTENTS

SEMO : Security Monitoring Platform

03 프로젝트 시연

프로젝트 시연 영상

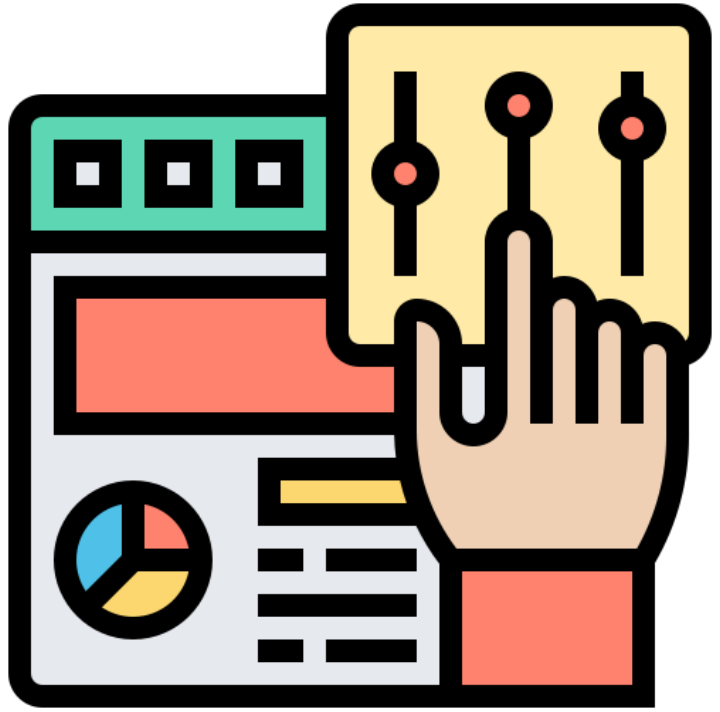


CONTENTS

SEMO : Security Monitoring Platform

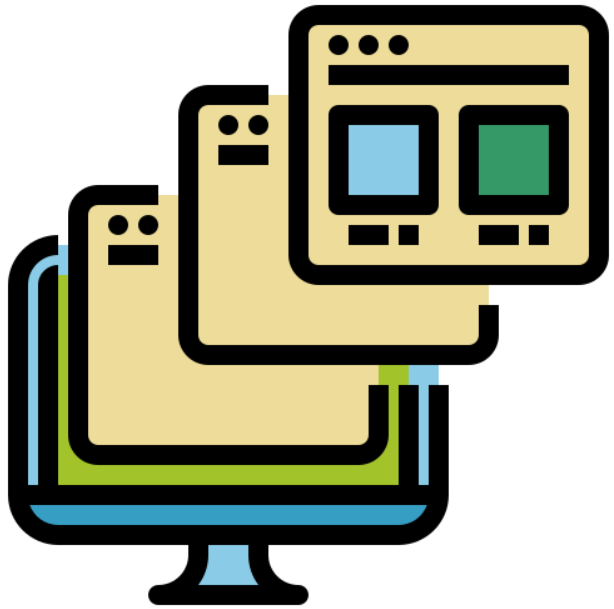
04 향후 계획

대시보드 가이드라인 제공



04 향후 계획

WEB Front-end 컨텐츠 추가



THANK YOU