2020 Capstone Design

SEMO : Security Monitoring Platform

CONTENTS

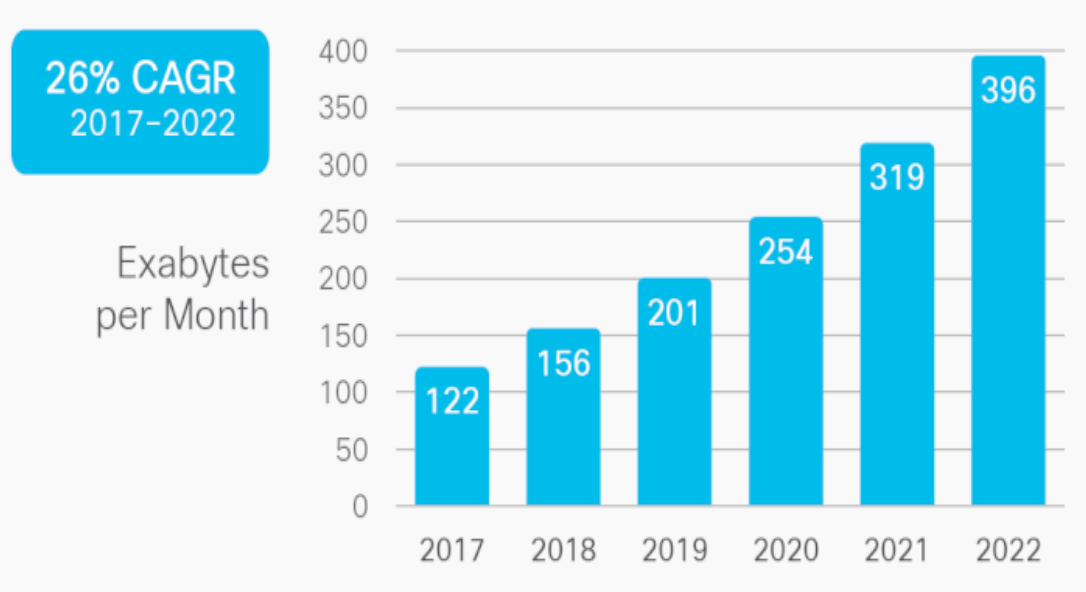
SEMO : Security Monitoring Platform

CONTENTS

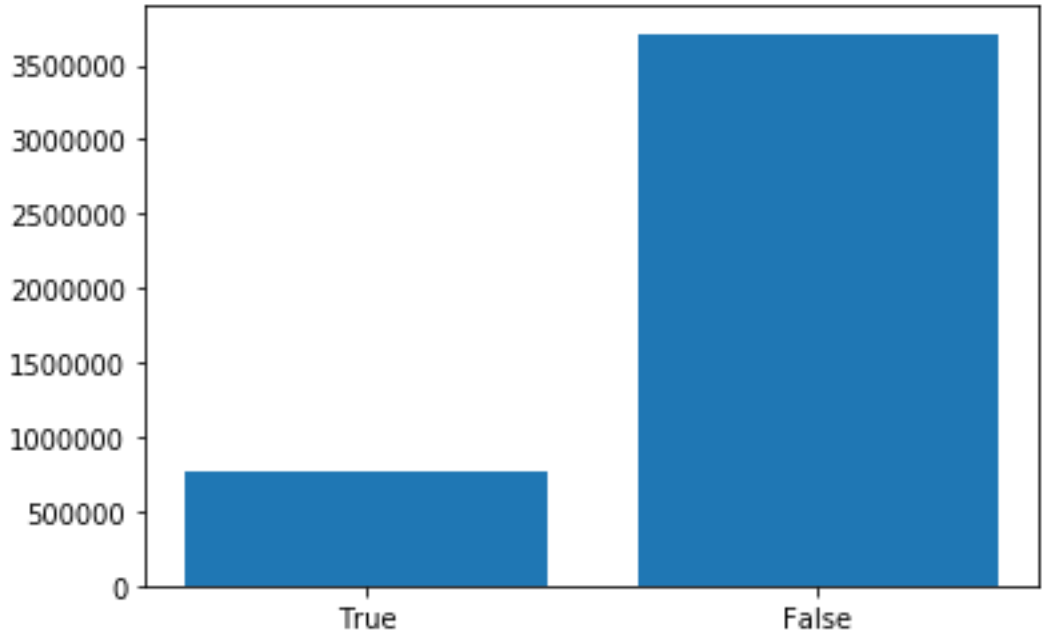
SEMO : Security Monitoring Platform

01 프로젝트 소개

증가하는 네트워크 트래픽



전세계 월별 IP 트래픽 전망
출처: Cisco VNI Global IP Traffic Forecast, 2017-2022



KISTI IPS Event Log 데이터 정탐/오탐 비율
출처: KISTI 사이버보안 안전센터

01 프로젝트 소개

현재 기술 시장의 문제점

전세계 월별 IP 트래픽 전망

출처: Cisco VNI Global IP Traffic Forecast, 2017-2022

KISTI IPS Event Log 데이터 정탐/오탐 비율

보안관제사들의 수동 정오탐 분류

일부 기업만 인공지능 도입

01 프로젝트 소개

프로젝트 목표

딥러닝을 통한 정오탐 분류 자동화

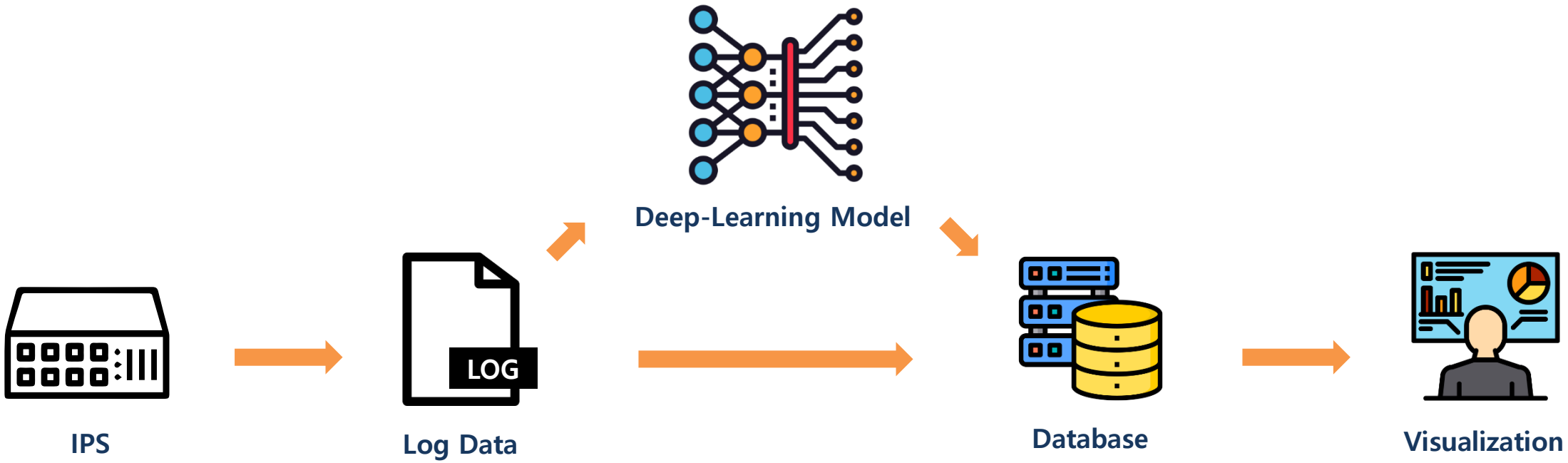
보안관제 플랫폼 구축 Best Practice 제공

CONTENTS

SEMO : Security Monitoring Platform

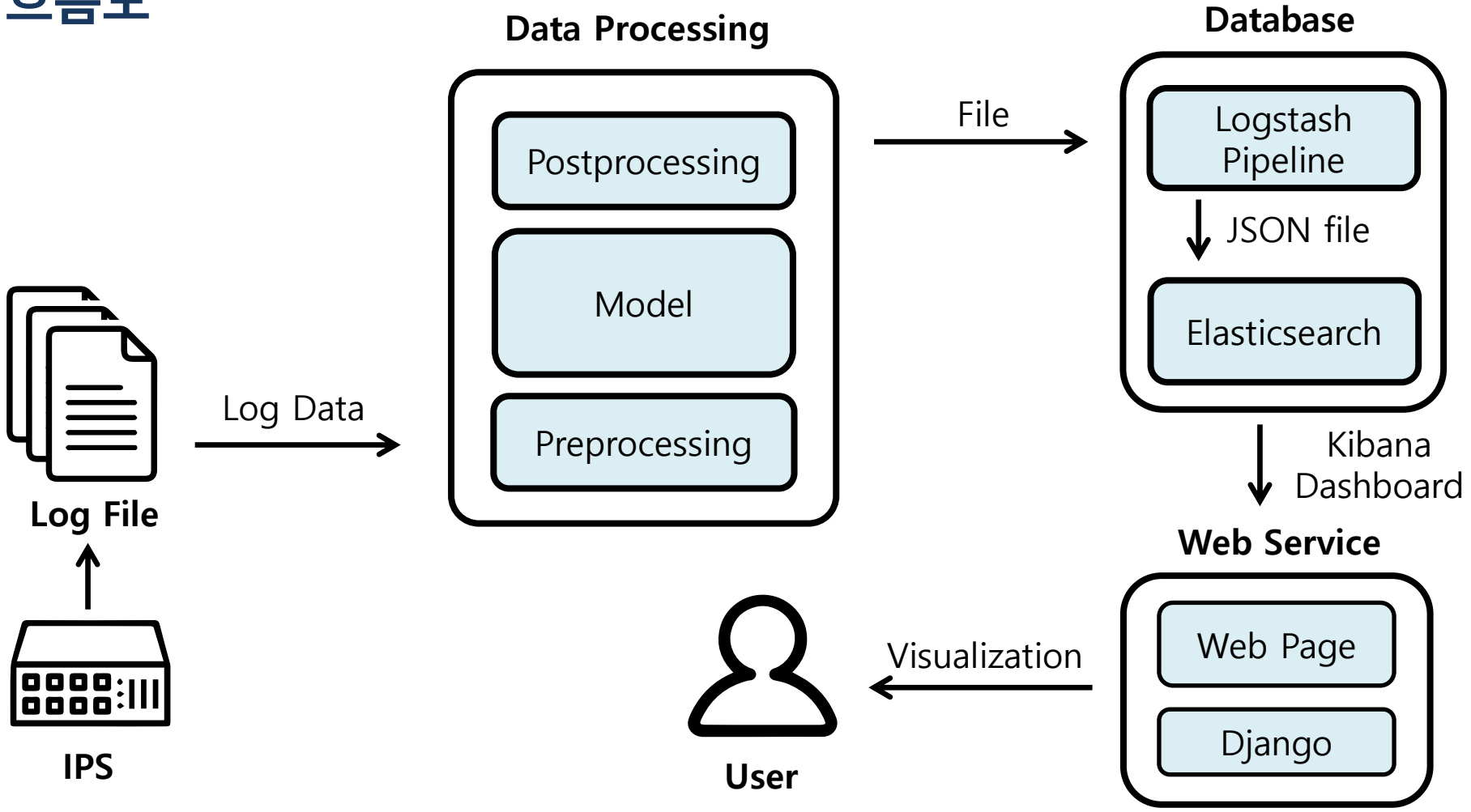
02 수행 내용

프로젝트 요약



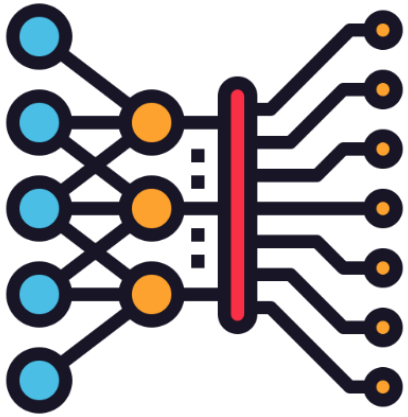
02 수행 내용

시스템 흐름도



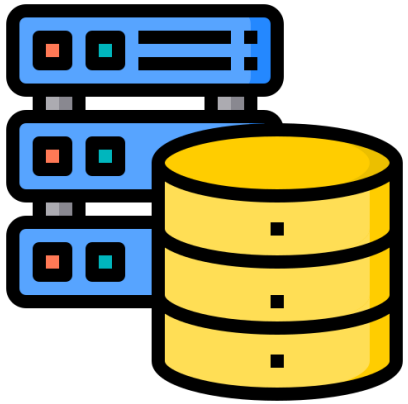
02 수행 내용

주요 기술



Model

- Conv Model



Database

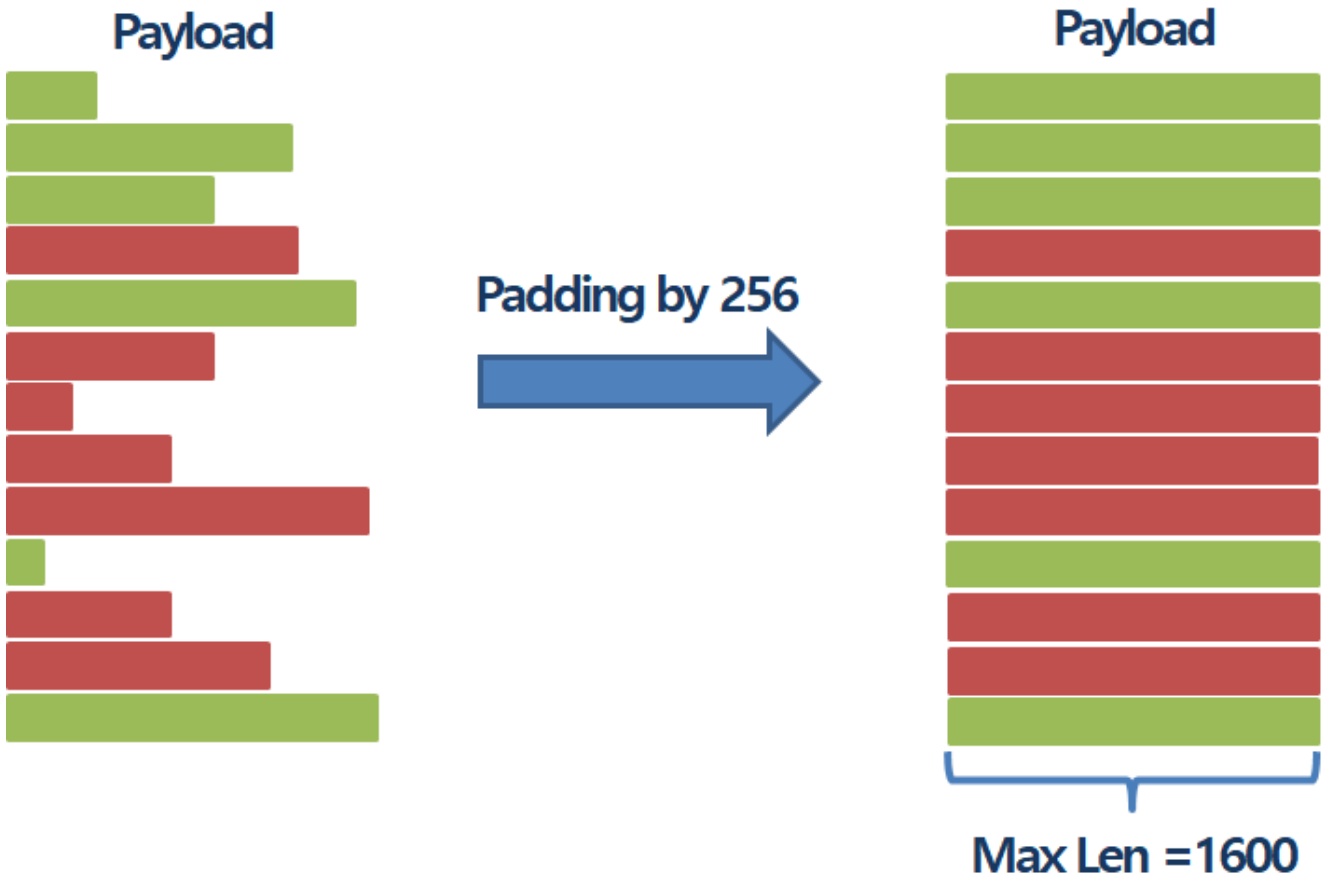
- Logstash
- Elasticsearch

Visualization

- Django
- Kibana

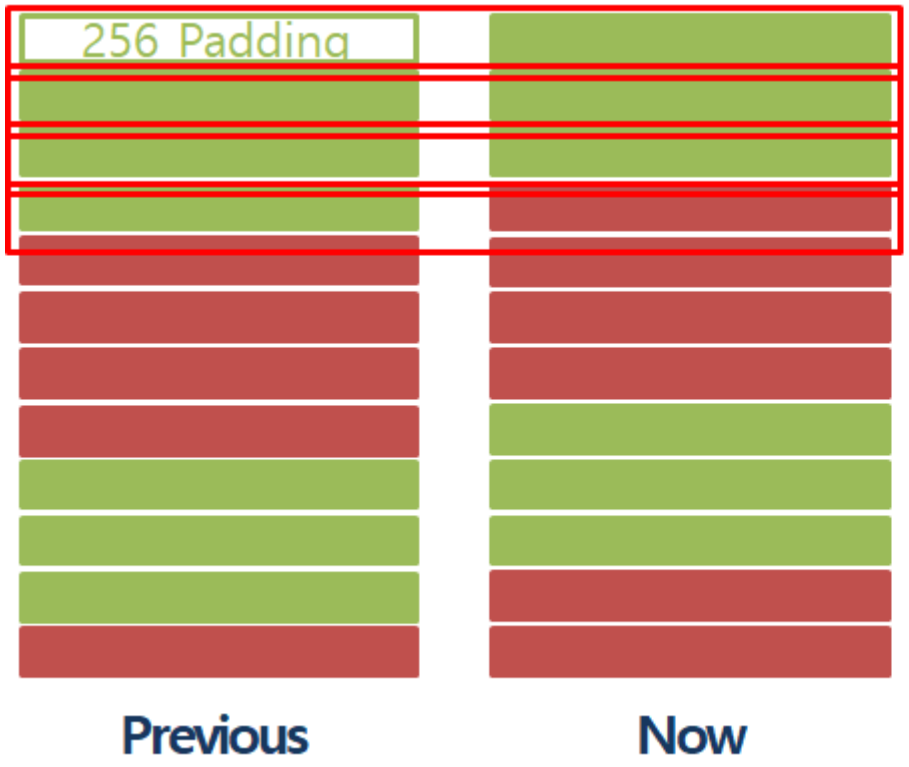
02 수행 내용

Model - 전처리 [Padding]



02 수행 내용

Model - 전처리 [Pre_Now]

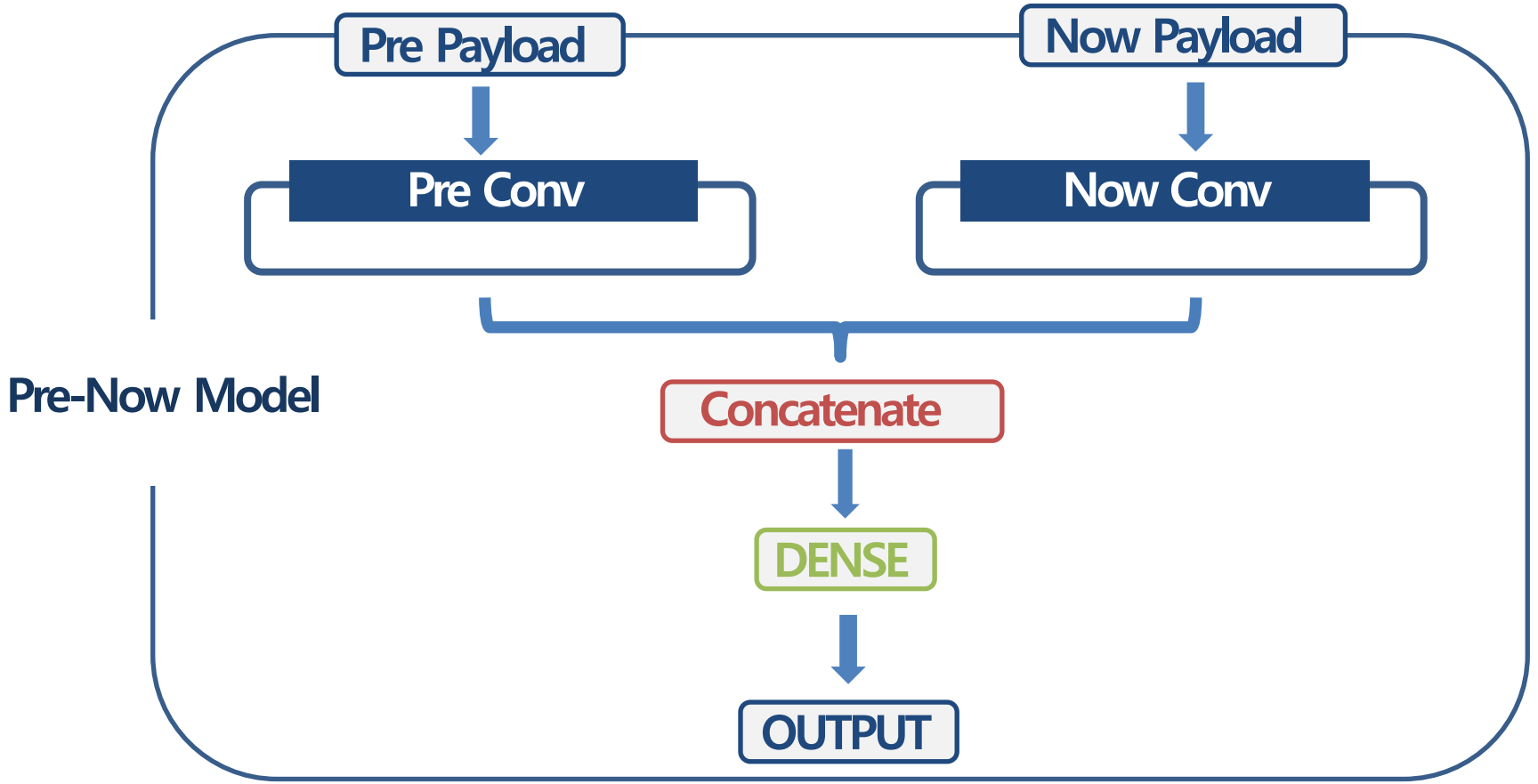


Data Input

➔ 현재 페이로드 학습 시
직전 페이로드 고려하여 학습

02 수행 내용

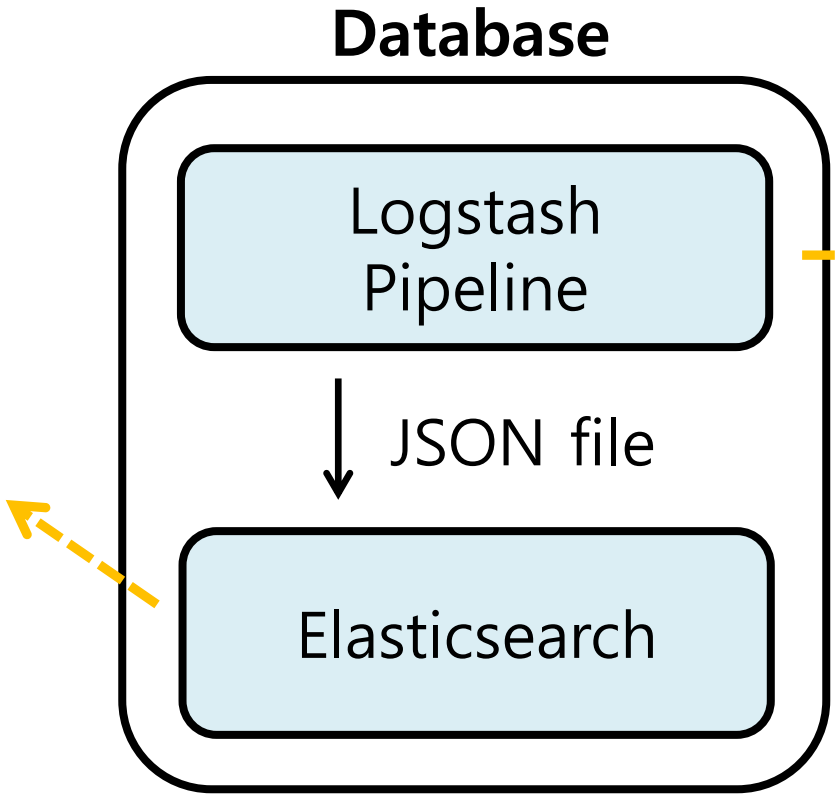
Pre_Now Model



02 수행 내용

Database – Elasticsearch & Logstash

Elasticsearch Data



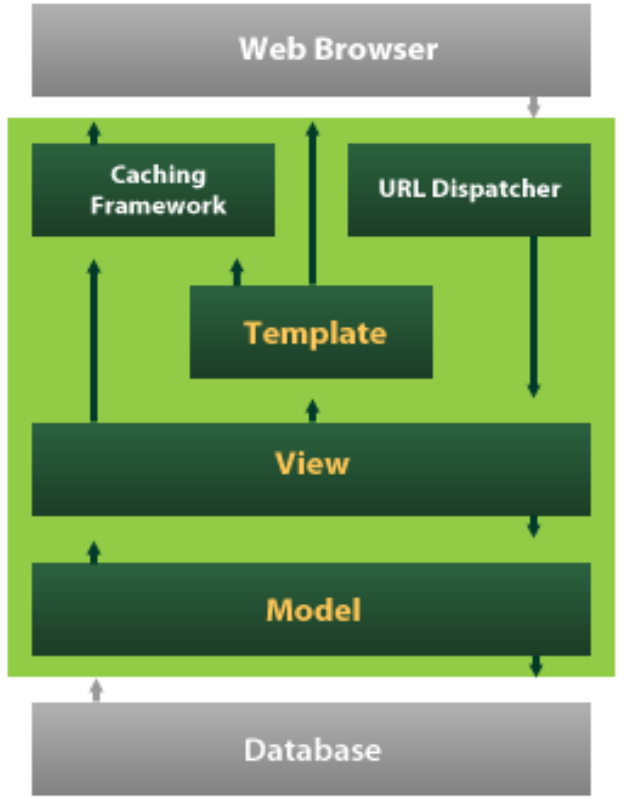

```
input {
 file {
   path => "file path"
   start_position => "beginning"
   sincedb_path => "/dev/null"
 }

}
filter {
 csv {
  separator => ","
  columns => ["id","uid","stdrPort","atdate","autoFlag","source
 }
 date{
  match => ["atdate", "yyyy-MM-dd HH:mm:ss.SSS"]
 }
 mutate {convert => ["stdrPort", "float"]}
 mutate {convert => ["sourcePort", "float"]}
 mutate {convert => ["eventType", "float"]}
 mutate {convert => ["accidentType", "float"]}
 mutate {convert => ["attackType", "float"]}
 mutate {convert => ["etcInfo", "float"]}
}
output {
 elasticsearch {
   hosts => ["http://localhost:9200"]
   index => "IndexToElasticsearch"
 }
 stdout{}
}
```

Logstash.conf

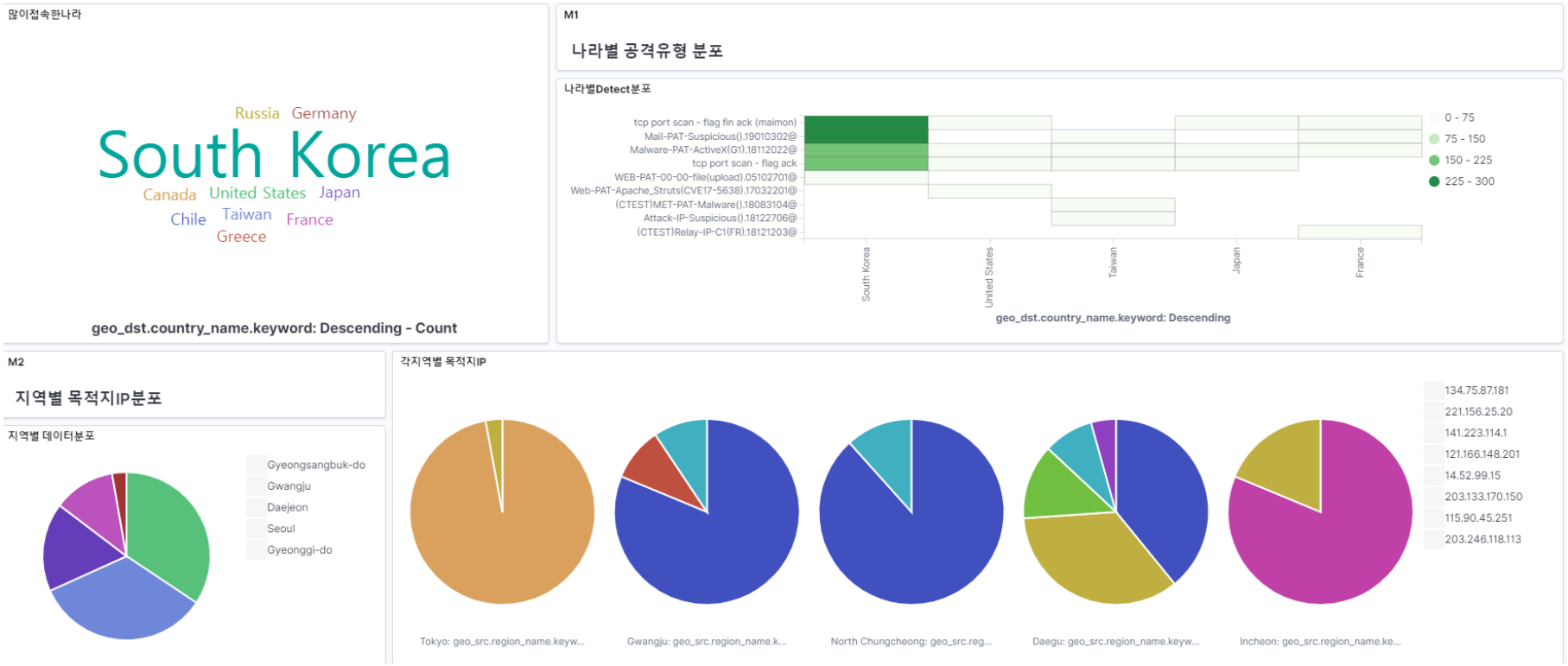
02 수행 내용

Visualization – Django(Web Service)



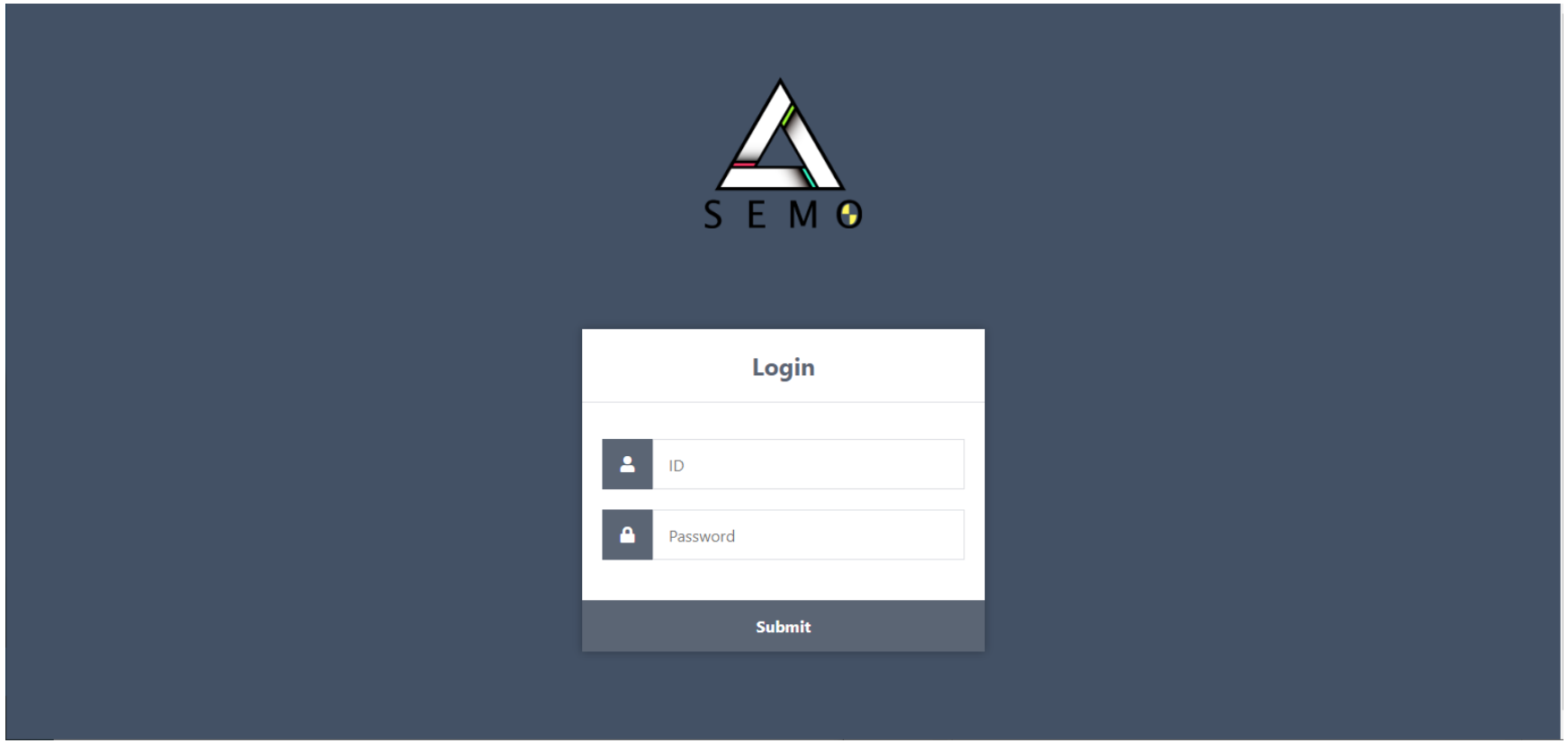
02 수행 내용

Visualization - Kibana Dashboard



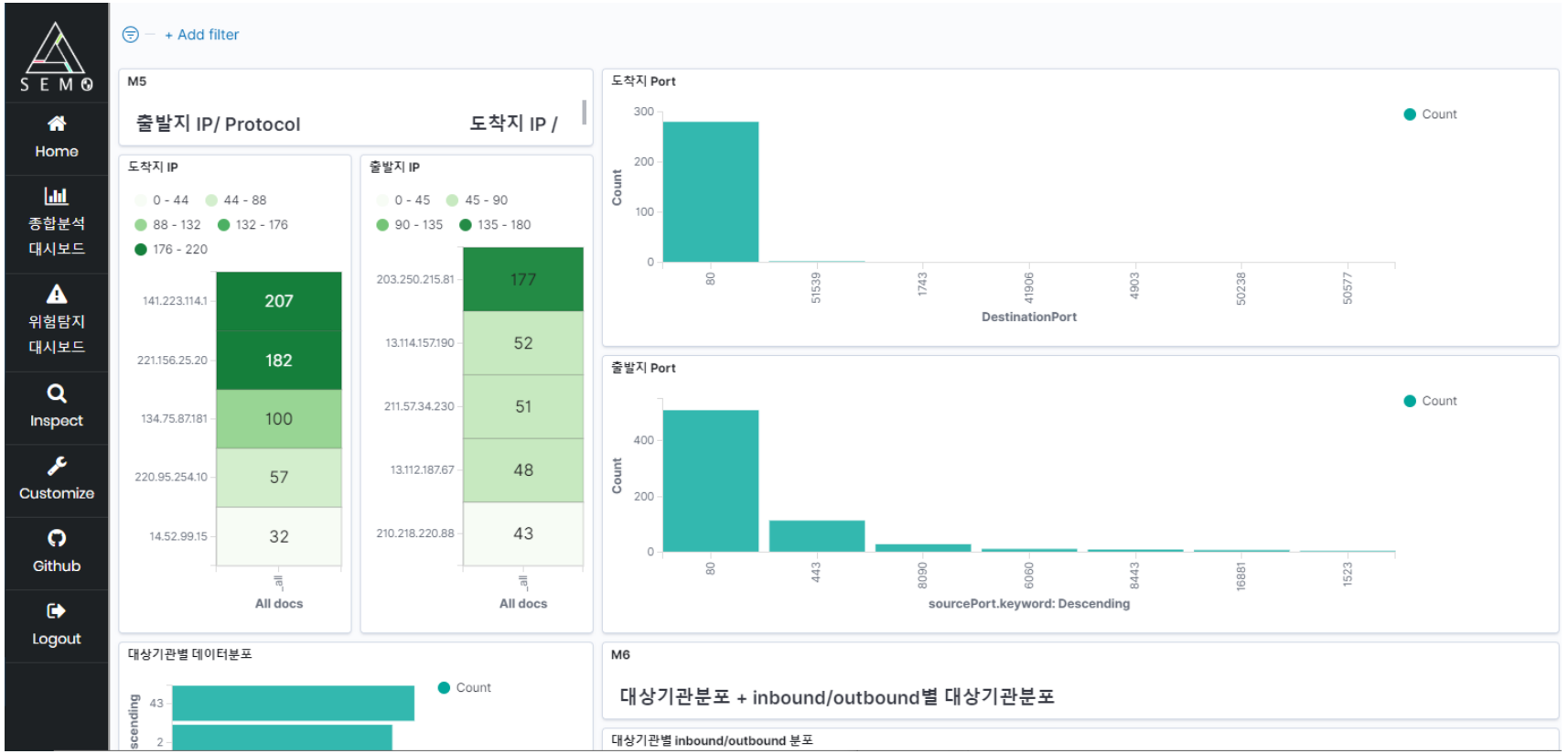
02 수행 내용

Visualization – Web Design



02 수행 내용

Visualization – Web Design



02 수행 내용

ELK 구축 가이드라인

ELK

해당 가이드라인은 ELK 스택 7.7 버전을 사용하였으며, 설치 및 사용에 관련된 내용은 버전별로 상이할 수 있습니다.

설치 순서

ELK Stack 설치 순서는 다음과 같습니다.

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

이 순서대로 설치하면 각 제품이 의존하는 구성 요소가 제 위치에 있게 됩니다.

Elasticsearch

```
sudo wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.7.0-linux-x86_64.tar.gz
sudo wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.7.0-linux-x86_64.tar.gz.sha512
shasum -a 512 -c elasticsearch-7.7.0-linux-x86_64.tar.gz.sha512
tar -xzf elasticsearch-7.7.0-linux-x86_64.tar.gz
```

refer by : https://www.elastic.co/guide/en/elasticsearch/reference/current/targz.html

Kibana

```
sudo curl -O https://artifacts.elastic.co/downloads/kibana/kibana-7.7.0-linux-x86_64.tar.gz
sudo curl https://artifacts.elastic.co/downloads/kibana/kibana-7.7.0-linux-x86_64.tar.gz.sha512 | shasum -a 512 -c -
tar -xzf kibana-7.7.0-linux-x86_64.tar.gz
```

Logstash

```
sudo curl -O https://artifacts.elastic.co/downloads/logstash/logstash-7.7.0.tar.gz
sudo curl https://artifacts.elastic.co/downloads/logstash/logstash-7.7.0.tar.gz.sha512 | shasum -a 512 -c -
tar -xvf logstash-7.7.0.tar.gz
```

kibana

kibana.yml

- kibana.yml example

실행 방법

https://github.com/kookmin-sw/capstone-2020-7/tree/feature/ELK/elk
위 설치 가이드라인을 따라 설치를 완료하였다면 실행방법은 다음과 같습니다.

```
[kibana 아카이브가 설치된 경로]/kibana-7.7.0-linux-x86_64/bin/kibana
```

Elasticsearch

elasticsearch.yml

- elasticsearch.yml guideline

실행 방법

https://github.com/kookmin-sw/capstone-2020-7/tree/feature/ELK/elk
위 설치 가이드라인을 따라 설치를 완료하였다면 실행방법은 다음과 같습니다.

```
[elasticsearch 아카이브가 설치된 경로]/elasticsearch-7.7.0/bin/elasticsearch
```

02 수행 내용

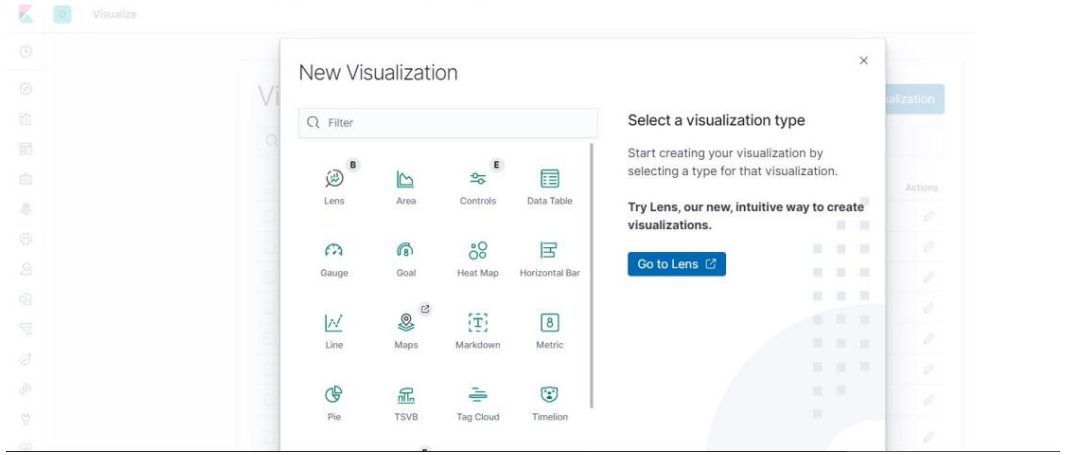
Kibana Dashboard 가이드라인

키바나 대시보드 만드는 큰순서

1. Discover -> change index pattern에서 대시보드를 만들 index설정 ->show dates에서 적절한 date범위 조절
2. Visualization -> create visualization ->시각화하고싶은 방법선택(ex:수직바차트,파이차트) -> data index 를 선택한다> 보이고 싶은 조건에 맞추어 구성
3. Dashboard -> create dashboard -> create new버튼으로 visualization 새로 생성 or add 버튼눌러서 만들어둔 visualization들 중 선택

Visualization 구성방법

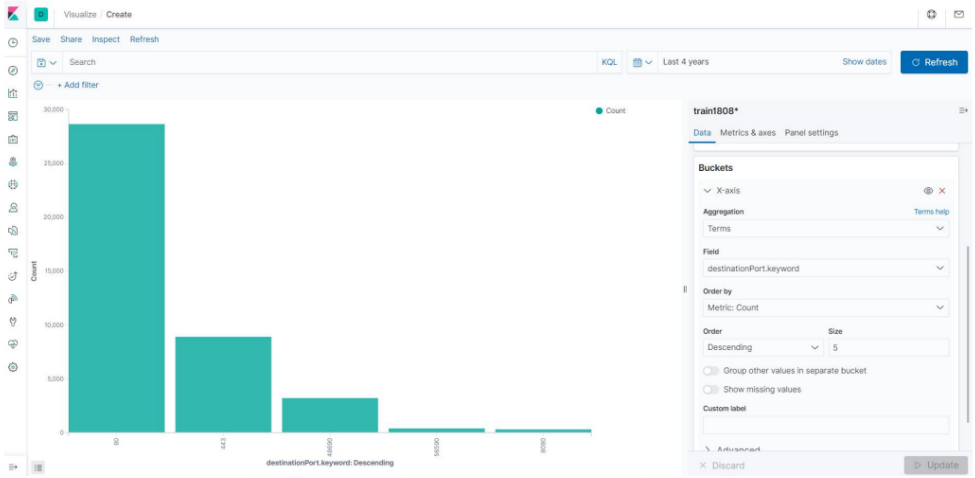
데이터 시각화를 시작하려면 사이드 탐색 메뉴에서 시각화 를 클릭합니다.



이번엔 Vertical Bar을 사용하여 데이터를 살펴보도록 하겠습니다.

(Pie chart의 슬라이스 = x axis 으로 조건을 나누는부분은 동일합니다)

1. 새로 만들기 를 클릭하고 'Vertical Bar'를 선택합니다.
2. Index 패턴을 선택합니다. 아직 어떤 버킷도 정의하지 않았으므로 커다란 하나의 바가 나타나 총 문서 수를 표시합니다.
3. Metric 집계의 y-axis에서 개수가 디폴트로 지정되어 있습니다. 만약 Max, Average, Min등 갯수가아닌 기준으로 바차트를 보이고싶다면 선택해줍니다. 예시에서는 count를 선택하였습니다.
4. X축을 설정해주기위해서는 Bucket -> X-axis을 선택한다음 agrregation에서 Terms을 선택해줍니다. 파이차트와 바차트에서는 주로 갯수를 보기위해 많이 쓰이므로 대부분 Terms를 사용합니다.
5. 앞서 보았던 파이차트와 동일하게 Order by, Order를 지정해줍니다. (만약 갯수가 아니라 알파벳순으로 나열하고싶다면 order by: Alphabetical로 설정해줍니다.



CONTENTS

SEMO : Security Monitoring Platform

03 기대 효과

기대효과

딥러닝을 통한 정오탐 분류 자동화

→ 보안관제사들의 능률 상승

보안관제 플랫폼 구축 Best Practice 제공

→ 딥러닝 기반 보안관제 서비스의 보편화

THANK YOU