<키바나 메뉴얼>

1. kibana 장점 (사용이유) / 2. 프로젝트에 사용한 기술 / 3. 설정방법

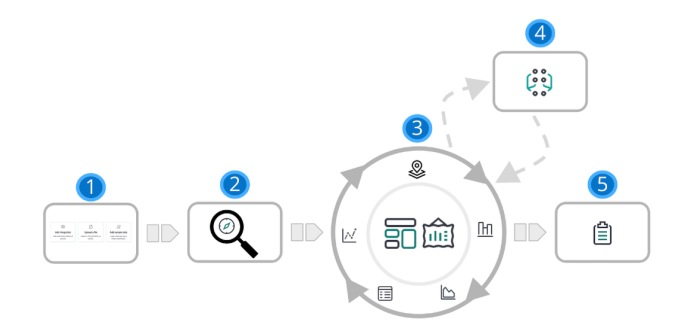
1. **키바나 장점(사용이유)**

Kibana는 Elasticsearch 데이터를 시각화하고 분석하는 데 최적화된 도구로, 실시간으로 데이터를 탐색하고 대시보드를 구성할 수 있는 다양한 기능을 제공

1. **직관적인 데이터 시각화**: 다양한 차트, 그래프, 지리 정보 시각화 등을 활용해 데이터를 쉽게 시각화할 수 있고 드래그 앤 드롭 방식의 UI를 통해 누구나 손쉽게 대시보드를 구성할 수 있음
2. **실시간 데이터 분석**: 실시간으로 데이터를 검색하고 분석할 수 있어, 시스템 상태와 사용자 활동을 즉각적으로 파악하고 대응할 수 있음. 이를 통해 더 빠르고 정확한 의사결정이 가능
3. **강력한 대시보드 기능**: 사용자 맞춤형 대시보드를 제공하여, 다양한 데이터 소스를 통합하고, 중요한 메트릭을 한눈에 모니터링할 수 있음. 대시보드를 통해 팀 간의 공유 및 협업을 촉진
4. **경고 및 알림 시스템**: Elasticsearch와 연동되어 특정 조건이 발생할 때 경고와 알림을 설정할 수 있음. 문제를 조기에 발견하고 대응할 수 있는 능력을 제공
5. **확장성과 통합성**: Elasticsearch와 완벽하게 통합되어 있어, 데이터의 수집, 검색, 분석이 매끄럽게 이루어짐. 또한, 다양한 플러그인과 통합을 통해 기능 확장도 가능
6. **사용자 친화적인 인터페이스**: 복잡한 데이터 분석 작업도 손쉽게 수행할 수 있도록 직관적이고 사용자 친화적인 인터페이스를 제공. 초보자부터 전문가까지 모두가 활용할 수 있는 유연성

이러한 Kibana의 장점을 바탕으로, 데이터 기반 의사결정에 필요한 강력한 시각화 및 분석 도구로 활용함

1. Kibana 데이터 분석 구성단계



1. 데이터 추가하기 (Add Data)

- 데이터 추가 방법 :

1) Elastic Stack 통합 기능 사용 2) 샘플 데이터 세트 추가 3) 파일 업로드

2. 탐색하기 (Explore)

- 데이터를 검색하고 필터를 적용해 원하는 정보만 볼 수 있음

3. 시각화하기 (Visualize)

- Dashboard를 통해 막대 그래프, 원형 그래프, 지도, 시간 시리즈 그래프 등으로 시각화

4. 데이터 행동 모델링 (Model Data Behavior)

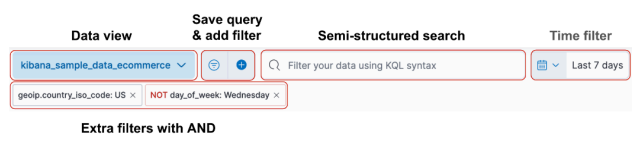
- Machine Learning을 통해 "보통"과 다른 "이상한" 패턴을 찾아내고 이후 상황에 대한 데이터를 예측

- 특정 부분이 다른 데이터 탐지(이상치 탐지), 예측 모델(회귀 분석), 카테고리 분류(분류 분석) 등을 작업

5. 공유하기 (Share)

- 대시보드를 웹사이트에 삽입하거나, 링크 공유, PDF로 내보낼 수 있음

1. **키바나 사용방법**
2. 데이터 검색방법



1. 검색 쿼리(Search Queries)

- 특정 조건에 맞는 데이터 검색 가능

2. 시간 필터(Time Filter)

- 특정 기간에 해당하는 데이터를 찾는데 사용

- 최근 7일 동안의 데이터를 보고 싶다면, 시간 필터를 사용해서 "지난 7일"을 선택

3. 반구조적 검색과 추가 필터(Semi-Structured Search and Extra Filters)

- 특정 필드와 그에 해당하는 값을 지정해서 검색

- 특정 키워드를 포함하는 데이터만 출력하는 등 검색 결과를 더욱 좁히고 싶을 때 사용

1. 데이터 뷰(Data Views)

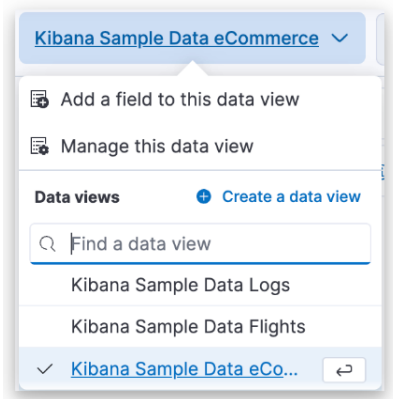
Kibana가 Elasticsearch에서 어떤 데이터를 가져와야 하는지 알려주는 지도로 다양한 데이터 스트림이나 인덱스에서 데이터를 검색하고, 필요한 필드의 형식과 이름으로 설정 가능

\* 생성한 데이터 뷰는 스택 관리(Stack Management)에서 관리

1. 데이터 뷰 만드는 방법

1) Lens 또는 Discover 열기

Kibana의 Lens 또는 Discover를 열고, 데이터 뷰 메뉴 열기



2) 데이터 뷰 생성 버튼 클릭

데이터 뷰 생성(Create a data view) 버튼 클릭

3) 데이터 뷰 이름 지정하기

새로 만들 데이터 뷰의 이름 입력

4) 인덱스 패턴 입력하기

Kibana가 입력한 내용과 일치하는 인덱스, 데이터 스트림, 별칭(alias) 이름을 찾을 수 있는 기능

○ 여러 소스를 매칭하려면 와일드카드(\*)를 사용

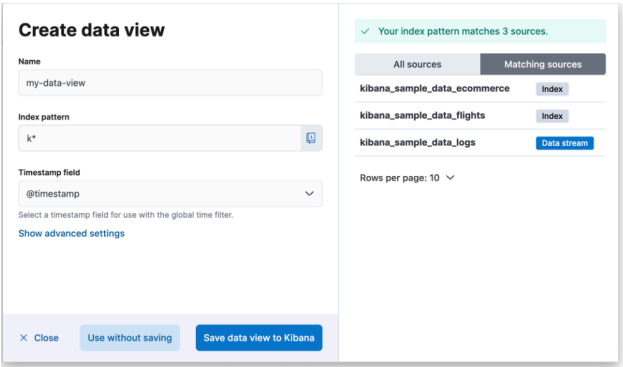
ex) filebeat-\* : filebeat-apache-a, filebeat-apache-b 등 여러 인덱스를 매칭

○ 여러 개의 단일 소스를 매칭하려면 인덱스 이름을 쉼표로 구분해서 입력(쉼표 뒤에 공백X)

ex) filebeat-a,filebeat-b : 두 개의 인덱스를 매칭

○ 특정 소스를 제외하려면 마이너스 기호(-)를 사용

ex) -test3 : test3 소스를 제외



5) 타임스탬프 필드 선택

"타임스탬프 필드(Timestamp field)" 드롭다운을 열고, 데이터를 시간별로 필터링할 기본 필드를 선택

○ 기본 시간 필드를 설정하지 않으면, 대시보드에서 전역 시간 필터를 사용할 수 없음

- 여러 시간 필드가 있을 때, 다른 타임스탬프에 기반한 시각화를 결합한 대시보드를 만들고 싶을 때 유용

○ 인덱스에 시간 기반 데이터가 없는 경우, \*\*시간 필터를 사용하고 싶지 않음(I don’t want to use the time filter)\*\*을 선택

6) 고급 설정 보기

다음의 내용 설정 가능

○ 숨겨진 인덱스와 시스템 인덱스를 표시

○ 데이터 뷰 이름 지정

7) 데이터 뷰 저장

데이터 뷰를 Kibana에 저장(Save data view to Kibana) 버튼 클릭

1. 대시보드에 시각화 패널 만드는 방법

1. 편집 모드로 전환하기

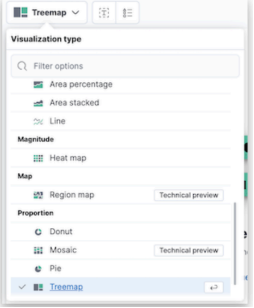
도구 모음에서 편집(Edit) 버튼 클릭

2. 새 시각화 만들기

대시보드에서 시각화 생성(Create visualization) 버튼 클릭

3. 트리맵 시각화 유형 선택

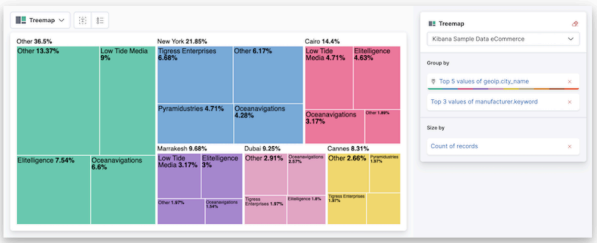
드래그 앤 드롭(Drag-and-Drop) 시각화 편집기 -> 시각화 유형(Visualization type) -> 트리맵(Treemap) 선택



4. 필드를 작업 공간으로 끌어오기

사용 가능한 필드 목록(Available fields list)에서 다음 필드를 작업 공간으로 드래그

ex) ■ geoip.city\_name : 도시 이름 ■ manufacturer.keyword : 제조사 키워드



5. 저장하고 돌아가기

저장 후 돌아가기(Save and return) 버튼 클릭