## Kibana란 무엇인가요?

**Kibana(키바나)**는 데이터를 더 쉽게 이해하고 사용할 수 있게 도와주는 도구예요. 데이터를 보고, 분석하고, 관리할 수 있는 창문 같은 역할을 해요. 데이터를 마치 마법처럼 모아서 필요한 정보를 찾아낼 수 있게 해주죠!

## Kibana로 할 수 있는 일

1. 데이터를 검색하고 관찰하고 보호하기
    - 예시: 만약 학교 도서관에 있는 모든 책의 목록이 있다면, 이 목록을 통해 어떤 책이 있는지 검색할 수 있죠. Kibana도 비슷해요. 회사나 학교에서 모은 데이터(예: 문서, 로그, 보안 정보 등)를 검색하고 분석할 수 있어요.
    - 예를 들어, 로그 데이터를 분석해서 시스템에 문제가 있는지 찾거나, 보안에 위협이 되는 부분을 발견할 수 있어요.
2. 데이터 분석 및 시각화
    - 예시: 친구들과 함께 놀이터에서 공을 몇 번 찼는지 기록했어요. 이 기록을 바탕으로 "누가 가장 많이 찼는지", "어떤 날에 공을 더 많이 찼는지"를 알 수 있는 차트를 만들 수 있어요. Kibana는 이런 작업을 도와주는 도구예요.
    - 데이터를 차트, 지도, 그래프 등으로 시각화해서 더 쉽게 이해할 수 있게 해줘요. 그리고 이 시각화된 데이터를 모아 대시보드라는 화면에 한눈에 볼 수 있게 정리해요.
3. Elastic Stack 관리, 모니터링, 보안
    - 예시: 집에서 아빠가 전구가 잘 켜지는지 확인하고, 창문이 잘 잠겨 있는지 보고, 집안 전체를 관리하시는 것처럼, Kibana도 데이터를 저장하는 시스템을 잘 관리하고 모니터링할 수 있도록 도와줘요.
    - 데이터가 잘 들어오는지 확인하고, 시스템의 건강 상태를 체크하고, 누가 어떤 기능을 사용할 수 있는지 설정할 수 있어요.

## 누가 Kibana를 사용할까요?

- 관리자(Admins): Kibana를 사용해서 전체 시스템을 관리하고, 데이터를 Elasticsearch로 가져와 정리하고, 시스템을 모니터링해요. 예를 들어, 선생님이 학교의 모든 책을 관리하고 정리하는 역할을 하는 것과 비슷해요.
- 분석가(Analysts): 데이터를 분석하고, 차트를 만들고, 대시보드를 구성해서 다른 사람들과 공유해요. 예를 들어, 친구들 사이에서 "어떤 날에 가장 많이 놀았는지"를 분석해서 알려주는 친구 같은 역할이죠.
- 비즈니스 사용자(Business Users): 이미 만들어진 대시보드를 보고, 필요한 정보를 찾아보고, 깊이 있는 분석을 해요. 예를 들어, 엄마가 학교에서 받은 성적표를 보고, 어떤 과목을 더 공부해야 할지 결정하는 것처럼요.

## 어떤 데이터를 Kibana에서 사용할 수 있을까요?

Kibana는 모든 종류의 데이터와 함께 사용할 수 있어요! 예를 들면:

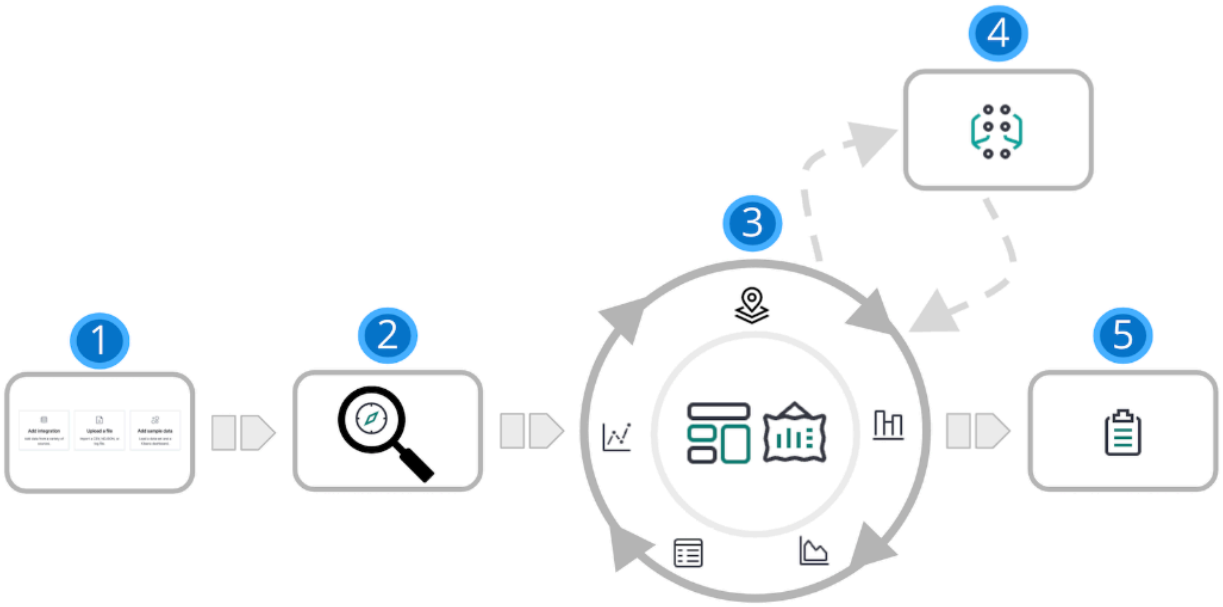
- 구조화된 데이터: 표처럼 깔끔하게 정리된 데이터 (예: 성적표, 쇼핑 목록)
- 비구조화된 텍스트: 깔끔하게 정리되지 않은 글 (예: 일기, 이메일)
- 숫자 데이터: 수치로 된 데이터 (예: 온도, 판매량)
- 시간 데이터: 시간이 중요한 데이터 (예: 매일의 날씨 기록, 주식 가격)
- 지도 데이터: 위치와 관련된 데이터 (예: 지도에서 특정 장소 표시하기)
- 로그 데이터: 컴퓨터나 서버에서 나오는 기록 (예: 컴퓨터가 언제 켜졌고 꺼졌는지)
- 보안 이벤트: 보안과 관련된 데이터 (예: 누가 컴퓨터에 로그인했는지)

결론

Kibana는 데이터를 보고 이해하는 것을 도와주는 멋진 도구예요. 마치 데이터로 가득 찬 큰 도서관에 창문을 달아, 그 안에서 어떤 책이 어디에 있는지 쉽게 찾을 수 있도록 해주는 것과 같아요. 데이터의 종류에 상관없이, Kibana는 우리가 필요로 하는 정보를 찾고, 분석하고, 시각적으로 표현할 수 있게 도와줘요!

## Kibana Analytics로 데이터 분석하기

Kibana는 데이터를 분석하고, 시각화하고, 공유할 수 있는 멋진 도구예요. 데이터를 쉽게 이해할 수 있게 차트나 그래프로 만들어주는 도구라고 생각하면 돼요. 여기서 Kibana가 제공하는 주요 기능들을 단계별로 설명해볼게요.




**1.** 데이터 추가하기 **(Add Data)**

먼저, 분석하고 싶은 데이터를 Kibana에 추가해야 해요.

- 예시: 학교에서 친구들의 키와 몸무게를 조사해서 수집했다고 생각해보세요. 이 데이터를 Kibana에 추가하면, 나중에 키와 몸무게의 관계를 분석할 수 있어요.
- 데이터를 추가하는 방법은 세 가지예요: Elastic Stack의 통합 기능을 사용하거나, 샘플 데이터 세트를 추가하거나, 파일을 업로드할 수 있어요. 이런 옵션들은 Kibana의 홈 페이지에서 사용할 수 있어요.

**2.** 탐색하기 **(Explore)**

Kibana의 **Discover** 기능을 사용하면 데이터를 자세히 탐색할 수 있어요.

- 예시: 친구들의 키와 몸무게 데이터를 탐색하면서, "가장 키가 큰 친구는 누구일까?" 또는 "가장 평균에 가까운 키는 얼마나 될까?" 같은 질문에 대한 답을 찾는 거예요.
- 데이터를 검색하고 필터를 적용해 원하는 정보만 볼 수 있어요. 예를 들어, 최근에 추가된 데이터만 보고 싶을 때 사용할 수 있어요.

**3.** 시각화하기 **(Visualize)**

데이터를 이해하기 쉽게 만들려면, 차트나 그래프 같은 시각화가 필요해요.

- 예시: 친구들의 키와 몸무게를 표나 그래프로 그려보면, 누가 더 크고 누가 더 작은지 쉽게 알 수 있겠죠? Kibana는 막대 그래프, 원형 그래프, 지도, 시간 시리즈 그래프 등 다양한 시각화 옵션을 제공해요.
- **Dashboard**를 사용하면 여러 시각화를 한 곳에 모아서 다양한 시각에서 데이터를 볼 수 있어요. **Canvas** 기능을 사용하면 큰 화면에서 멋진 시각화를 보여줄 수 있고, **Graph** 기능을 사용해 패턴과 관계를 탐구할 수 있어요.

**4.** 데이터 행동 모델링 **(Model Data Behavior)**

Kibana는 **Machine Learning(기계 학습)**을 사용하여 데이터의 행동을 모델링할 수 있어요.

- 예시: 만약 친구들의 키가 갑자기 빠르게 자라기 시작한다면? Kibana의 기계 학습 기능을 사용해 "보통"과 다른 "이상한" 패턴을 찾아낼 수 있어요. 그리고 미래에 있을 가능성이 있는 데이터를 예측할 수도 있어요.
- 또한, 데이터의 특정 부분이 다른 것들과 다른지(이상치 탐지), 예측 모델(회귀 분석), 카테고리 분류(분류 분석) 등을 할 수 있어요.

**5.** 공유하기 **(Share)**

분석한 결과를 다른 사람들과 공유할 수 있어요.

- 예시: 친구들과 키와 몸무게에 대한 분석 결과를 공유하고 싶다면, Kibana를 사용해서 대시보드를 웹사이트에 삽입하거나, 링크로 공유하거나, PDF로 내보낼 수 있어요.
- 이를 통해 분석한 결과를 더 많은 사람들과 쉽게 공유할 수 있어요.

요약

- 데이터 추가**(Add Data)**: 분석하고 싶은 데이터를 추가해요.
- 탐색**(Explore)**: 데이터를 탐색하고 숨겨진 정보를 찾아내요.
- 시각화**(Visualize)**: 데이터를 그래프나 차트로 시각화해서 쉽게 이해할 수 있도록 해요.
- 데이터 행동 모델링**(Model Data Behavior)**: 기계 학습을 통해 데이터를 분석하고 미래를 예측해요.
- 공유**(Share)**: 분석한 결과를 다른 사람들과 공유해요.

Kibana를 사용하면 복잡한 데이터도 쉽게 분석하고, 시각화하고, 공유할 수 있어서 마치 데이터를 다루는 마법사가 된 것 같은 기분이 들 거예요!

## Kibana에서 데이터 접근하기**: **데이터 뷰**(Data Views)****란?

Kibana는 데이터를 보기 위해 **데이터 뷰(Data Views)**라는 것을 사용해요. 데이터 뷰는 Kibana에게 "어떤 데이터를 보고 싶은지"와 "그 데이터가 시간과 관련이 있는지"를 알려주는 역할을 해요. 마치 도서관에서 특정 주제의 책을 찾고 싶을 때, 사서에게 어떤 책을 찾고 싶은지 설명하는 것과 비슷해요!

**1.** 데이터 뷰란**?**

- **데이터 뷰(Data View)**는 Kibana가 Elasticsearch에서 어떤 데이터를 가져와야 하는지 알려주는 일종의 지도 같은 거예요.
- 이 데이터 뷰는 하나 이상의 데이터 스트림**(Data Stream)**, 인덱스**(Index)**, 또는 **인덱스 별칭(Index Alias)**에 해당하는 데이터를 가리킬 수 있어요.
    - 데이터 스트림: 계속해서 업데이트되는 데이터 흐름이라고 생각하면 돼요. 예를 들어, 매일매일 업데이트되는 날씨 정보 같은 거예요.
    - 인덱스: 책을 모아놓은 서가처럼, 특정한 데이터 종류를 모아놓은 곳이에요.
    - 인덱스 별칭: 별명처럼 여러 인덱스를 가리킬 수 있는 이름이에요. 한꺼번에 여러 서가를 가리키는 표지판과 같아요.

**2.** 데이터 뷰를 어떻게 만들까요**?**

- 데이터 뷰는 주로 관리자가 Elasticsearch에 데이터를 보낼 때 만들어요. 관리자는 어떤 데이터를 Kibana에서 보고 분석할지 결정하고, 그에 맞는 데이터 뷰를 만들어 주죠.
- 사용자는 **Stack Management**라는 Kibana의 설정 페이지에서 데이터 뷰를 만들거나 업데이트할 수 있어요. 또는, **Kibana API**를 이용한 스크립트를 통해 자동으로 데이터 뷰를 만들 수도 있어요.

**3.** 데이터 뷰로 무엇을 할 수 있나요**?**

- 필드 목록 보기: 데이터 뷰를 사용하면 Kibana는 우리가 사용할 수 있는 필드**(Fields)** 목록을 보여줘요. 필드는 데이터의 세부적인 항목이에요. 예를 들어, `event.duration`이라는 필드는 어떤 이벤트가 얼마나 오래 지속되었는지를 나타내요.

- 필드의 표시 이름과 형식 설정하기: 데이터가 더 쉽게 이해될 수 있도록 각 필드의 표시 이름과 형식을 사용자 맞춤으로 설정할 수 있어요.
    - 예시: `event.duration`이라는 필드가 있다면, Kibana에 이 값을 **초 단위(Seconds)**로 표시하라고 설정할 수 있어요. 이렇게 하면 우리가 데이터를 볼 때 더 쉽게 이해할 수 있죠.
    - Kibana는 문자열(String), 날짜(Date), 지리적 위치(Geopoints), 숫자(Number) 등 다양한 데이터 유형에 맞는 **필드 형식 지정자(Field Formatter)**를 가지고 있어요.

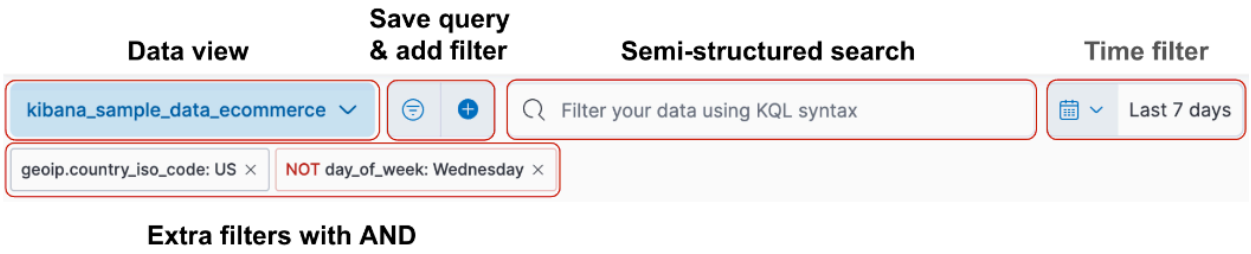
요약

- 데이터 뷰**(Data Views)**: Kibana에게 어떤 데이터를 가져와서 보여줄지 알려주는 지도와 같은 역할을 해요.
- 데이터 뷰를 사용하면, 다양한 데이터 스트림이나 인덱스에서 데이터를 검색하고, 필요한 필드의 형식과 이름을 사용자 맞춤으로 설정할 수 있어요.
- 이를 통해, 우리는 데이터를 더 쉽게 이해하고 분석할 수 있게 돼요.

Kibana에서 데이터를 더 효율적으로 활용하려면 데이터 뷰를 잘 사용하는 것이 중요해요!

## Kibana에서 데이터 검색하기

Kibana는 데이터를 쉽게 검색할 수 있도록 여러 가지 방법을 제공해요. 마치 도서관에서 원하는 책을 찾을 때, 책 제목, 저자 이름, 출판 연도 등을 사용해 검색하는 것과 비슷해요.




**1.** 검색 쿼리**(Search Queries)**

- 검색 쿼리는 Elasticsearch에서 원하는 데이터를 찾기 위해 사용하는 검색 명령어예요.
- 예시: 만약 도서관에서 "2022년에 출판된 책"이나 "작가가 '이영도'인 책"을 찾고 싶다면, 그런 조건을 검색하는 것과 같아요. Kibana에서도 비슷하게 특정 조건에 맞는 데이터를 찾기 위해 검색 쿼리를 사용할 수 있어요.

**2.** 시간 필터**(Time Filter)**

- Kibana의 많은 앱들은 시간 필터를 제공해요. 시간 필터는 특정 기간에 해당하는 데이터를 찾는 데 사용돼요.

- 예시: 최근 7일 동안의 데이터를 보고 싶다면, 시간 필터를 사용해서 "지난 7일"을 선택할 수 있어요. 마치 "지난주에 학교 도서관에 들어온 새 책만 보여줘"라고 요청하는 것과 비슷하죠.

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

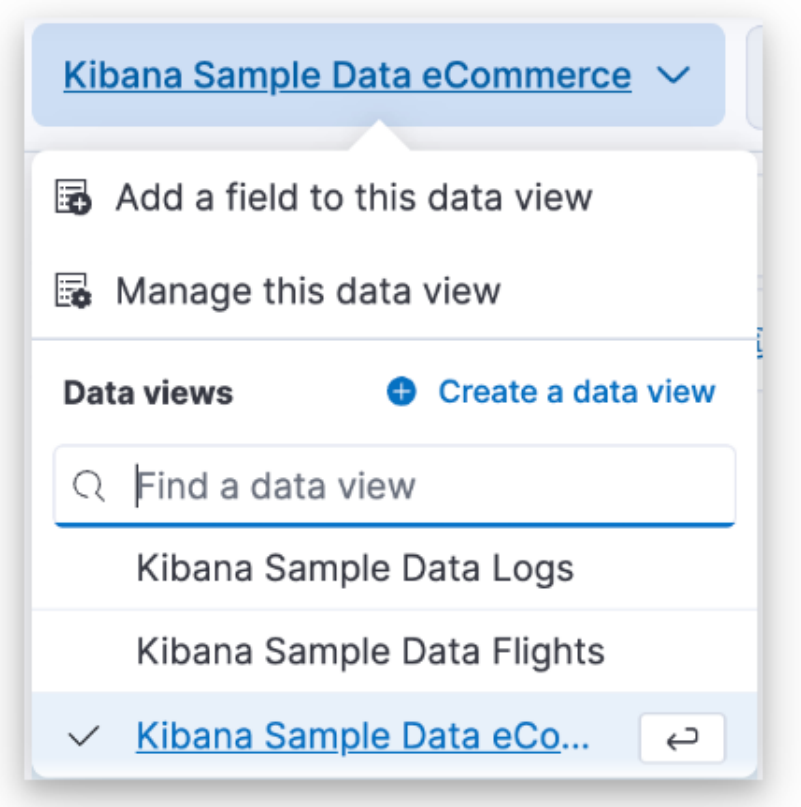
- 반구조적 검색은 데이터를 검색할 때, 특정 필드(예: 제목, 저자, 연도 등)와 그에 해당하는 값을 지정해서 검색할 수 있는 방법이에요.
- 추가 필터는 검색 결과를 더욱 좁히고 싶을 때 사용해요. 예를 들어, 특정 키워드를 포함하는 데이터만 보고 싶을 때 필터를 추가할 수 있어요.
- 예시: "2022년에 출판된 책" 중에서도 "과학" 카테고리에 속한 책만 보고 싶을 때, 반구조적 검색과 추가 필터를 사용할 수 있어요.

## 데이터 뷰 만들기

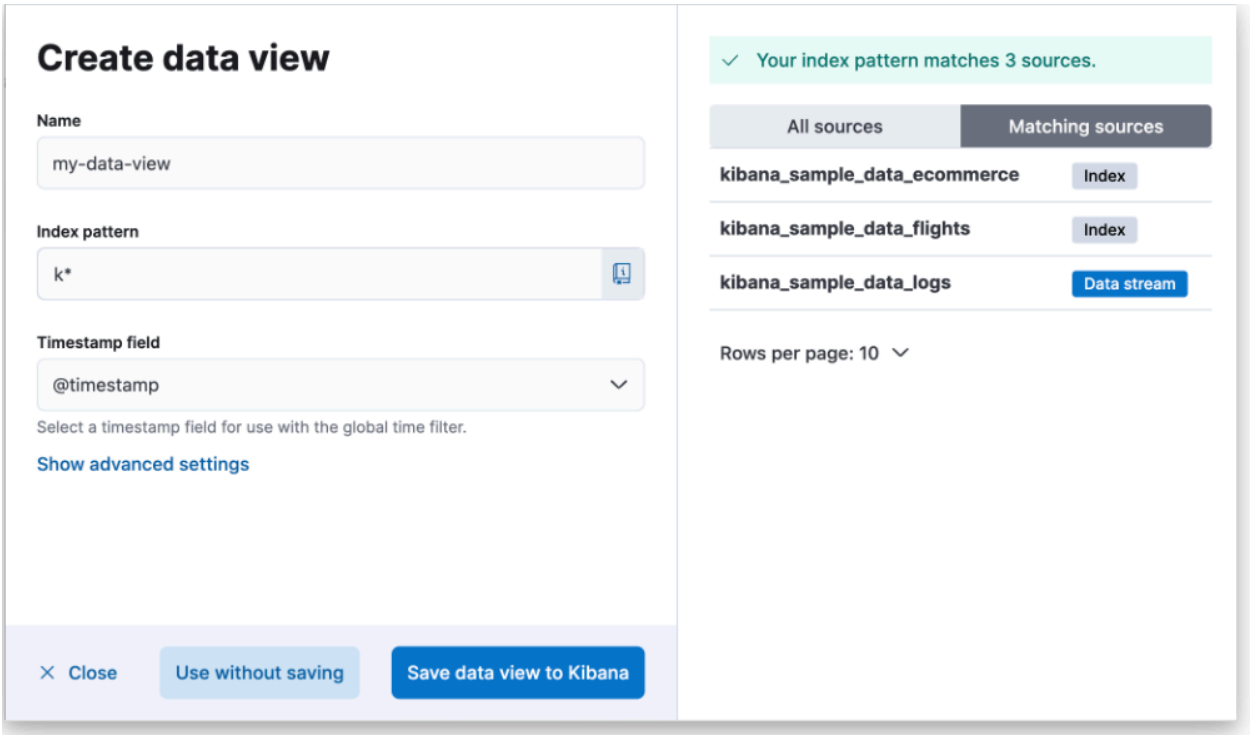
만약 Kibana의 데이터 수집 옵션을 사용하거나, 파일을 업로드하거나, 샘플 데이터를 추가한 경우, 기본적으로 데이터 뷰가 제공되어 바로 데이터를 탐색할 수 있어요. 그러나 자신만의 데이터를 로드한 경우, 다음 단계에 따라 데이터 뷰를 만들어야 해요.

데이터 뷰 만드는 방법

1. **Lens** 또는 **Discover** 열기
   Kibana의 Lens 또는 Discover를 열고, 데이터 뷰 메뉴를 엽니다.



2. 데이터 뷰 생성 버튼 클릭
   데이터 뷰 생성**(Create a data view)** 버튼을 클릭합니다.
3. 데이터 뷰 이름 지정하기
   새로 만들 데이터 뷰의 이름을 입력합니다.
4. 인덱스 패턴 입력하기
   "인덱스 패턴(Index pattern)" 필드에 입력을 시작하면 Kibana가 입력한 내용과 일치하는 인덱스, 데이터 스트림, 별칭(alias) 이름을 찾아줍니다. 모든 사용 가능한 소스를 보거나, 데이터 뷰가 타겟팅하는 소스만 볼 수 있어요.
   - 여러 소스를 매칭하려면 와일드카드(*)를 사용하세요. 예를 들어, `filebeat-*`는 `filebeat-apache-a`, `filebeat-apache-b` 등 여러 인덱스를 매칭합니다.
   - 여러 개의 단일 소스를 매칭하려면 인덱스 이름을 쉼표로 구분해서 입력하세요. 쉼표 뒤에 공백은 넣지 않습니다. 예를 들어, `filebeat-a,filebeat-b`는 두 개의 인덱스를 매칭합니다.
   - 특정 소스를 제외하려면 마이너스 기호(-)를 사용하세요. 예를 들어, `-test3`는 `test3` 소스를 제외합니다.




5. 타임스탬프 필드 선택
   "타임스탬프 필드(Timestamp field)" 드롭다운을 열고, 데이터를 시간별로 필터링할 기본 필드를 선택하세요.
   - 기본 시간 필드를 설정하지 않으면, 대시보드에서 전역 시간 필터를 사용할 수 없습니다. 여러 시간 필드가 있을 때, 다른 타임스탬프에 기반한 시각화를 결합한 대시보드를 만들고 싶을 때 유용합니다.

- 인덱스에 시간 기반 데이터가 없는 경우, **시간 필터를 사용하고 싶지 않음(I don't want to use the time filter)**을 선택하세요.

6. 고급 설정 보기
   **고급 설정 보기(Show advanced settings)**를 클릭하여 다음을 설정할 수 있습니다:
   - 숨겨진 인덱스와 시스템 인덱스를 표시합니다.
   - 자신만의 데이터 뷰 이름을 지정할 수 있습니다. 예를 들어, Elasticsearch 인덱스 별칭(alias) 이름을 입력합니다.
7. 데이터 뷰 저장
   데이터 뷰를 **Kibana**에 저장**(Save data view to Kibana)** 버튼을 클릭합니다.

데이터 뷰 관리

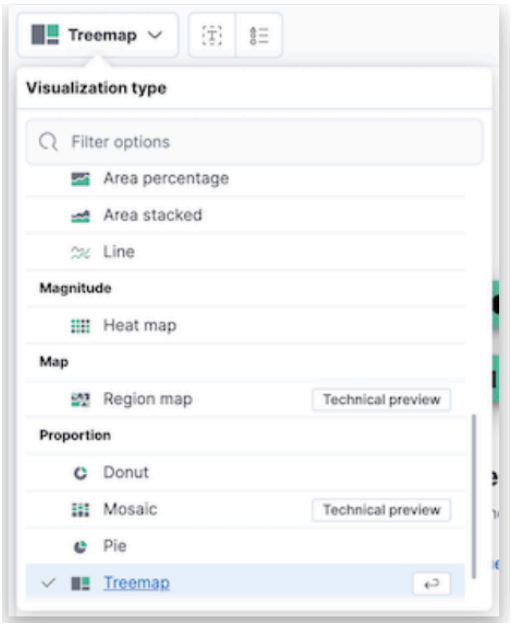
생성한 데이터 뷰는 **스택 관리(Stack Management)**에서 관리할 수 있습니다.

## 대시보드에 시각화 패널 만들기

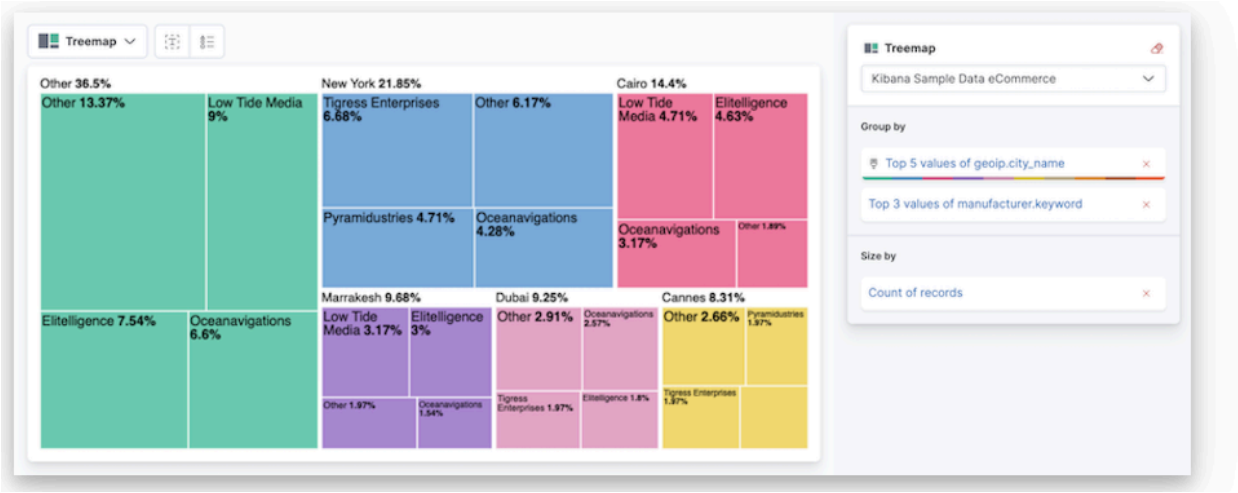
트리맵**(Treemap)** 시각화 패널을 만들어서 가장 높은 매출을 기록한 지역과 제조사**(**예시**)**를 보여주는 방법을 설명할게요. 그런 다음, 이 패널을 대시보드에 추가할 수 있습니다.

트리맵 시각화 패널 만들기

1. 편집 모드로 전환하기
   - 도구 모음에서 편집**(Edit)** 버튼을 클릭합니다.
2. 새 시각화 만들기
   - 대시보드에서 시각화 생성**(Create visualization)** 버튼을 클릭합니다.
3. 트리맵 시각화 유형 선택
   - 드래그 앤 드롭(Drag-and-Drop) 시각화 편집기에서 시각화 유형**(Visualization type)** 드롭다운을 열고, **트리맵(Treemap)**을 선택합니다.



4. 필드를 작업 공간으로 끌어오기
    - **사용 가능한 필드 목록(Available fields list)**에서 다음 필드를 작업 공간으로 드래그합니다:
        - `geoip.city_name` : 도시 이름
        - `manufacturer.keyword` : 제조사 키워드**(**예시**)**




5. 저장하고 돌아가기
    - 저장 후 돌아가기**(Save and return)** 버튼을 클릭합니다.