Modul 02: Discover & Abfragen

Daten durchsuchen, filtern und analysieren mit Kibana Discover

Lernziele

Nach diesem Modul kannst du:

- Die Discover-Oberfläche in Kibana sicher bedienen
- Zeitfilter gezielt einsetzen, um relevante Zeiträume auszuwählen
- Mit der Kibana Query Language (KQL) präzise Abfragen formulieren
- Filter kombinieren, um Datenbestände einzugrenzen
- Spalten konfigurieren und Dokumente im Detail untersuchen
- Ergebnisse als CSV exportieren und gespeicherte Suchen teilen

Kibana Discover - Überblick

Discover ist dein zentrales Werkzeug, um Daten in Elasticsearch zu durchsuchen und zu erkunden.

Typische Anwendungsfälle bei Mustertech GmbH:

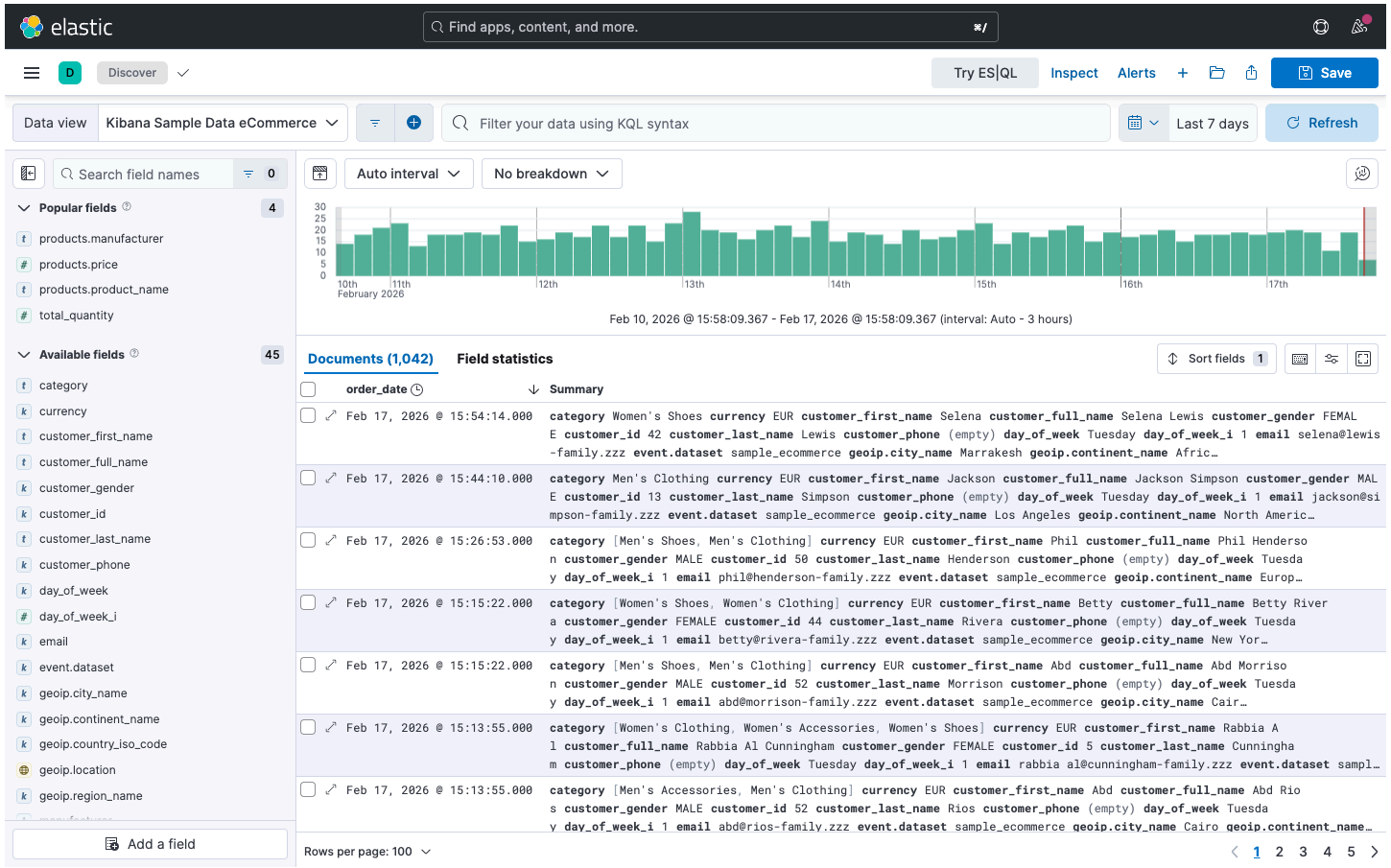
- Bestellungen eines bestimmten Zeitraums finden
- Umsätze nach Produktkategorie analysieren
- Kundenregionen auswerten
- Auffällige Bestellwerte identifizieren

> Discover zeigt dir die Rohdaten - hier beginnst du jede Analyse.

Die Discover-Oberfläche

Bereich	Beschreibung
Suchleiste	KQL-Abfragen eingeben
Zeitfilter	Zeitraum auswählen (oben rechts)
Histogramm	Verteilung der Treffer über die Zeit
Felderliste	Verfügbare Felder (linke Seitenleiste)
Dokumententabelle	Trefferliste mit konfigurierbaren Spalten
Dokumentendetails	Einzelnes Dokument aufklappen
Filter-Leiste	Aktive Filter unterhalb der Suchleiste

Die Discover-Oberfläche - Kibana



Data Views (ehemals Index Patterns)

Ein **Data View** legt fest, welche Elasticsearch-Indizes du durchsuchst.

Beispiele bei Mustertech GmbH:

- `mustertech-orders-*` -- alle Bestelldaten
- `mustertech-products-*` -- Produktkatalog
- `mustertech-customers-*` -- Kundendaten

So wählst du einen Data View aus:

1. Klicke oben links auf den Data-View-Namen
2. Wähle den gewünschten Data View aus der Liste
3. Die Felderliste und Daten aktualisieren sich automatisch

> Der Data View bestimmt, welche Felder dir zur Verfügung stehen.

Zeitfilter und Zeitreihen

Der Zeitfilter ist eines der wichtigsten Werkzeuge in Discover. Er befindet sich oben rechts in der Oberfläche.

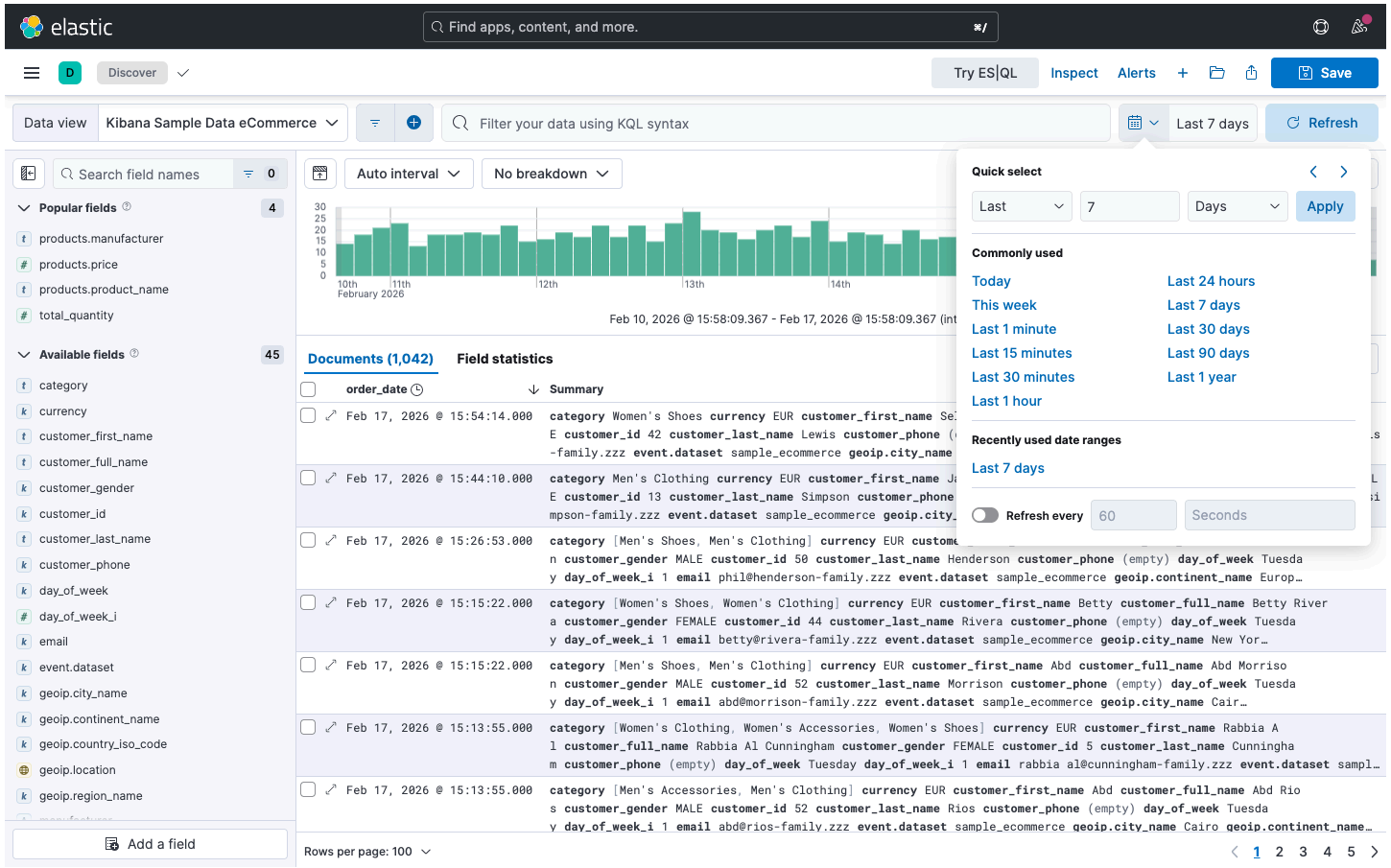
Zwei Arten der Zeitauswahl:

- **Relativ:** z. B. "Letzte 24 Stunden", "Letzte 7 Tage", "Letzte 30 Tage"
- **Absolut:** z. B. "01.01.2026 00:00" bis "31.01.2026 23:59"

Wann welche Variante nutzen?

Relativ	Absolut
Laufende Überwachung	Monatsberichte
Tagesaktuelle Analyse	Quartalsvergleiche
Dashboards mit Auto-Refresh	Reproduzierbare Auswertungen

Zeitfilter - Quick Menu



Das Histogramm nutzen

Das Histogramm oben in Discover zeigt die **Verteilung der Treffer über die Zeit**.

So nutzt du es effektiv:

- **Überblick verschaffen:** Erkenne auf einen Blick, wann besonders viele Bestellungen eingegangen sind
- **Hineinzoomen:** Klicke und ziehe, um einen Zeitbereich auszuwählen
- **Intervall anpassen:** Kibana wählt das Intervall automatisch, du kannst es aber manuell ändern (z. B. stündlich, täglich)

> Auffällige Spitzen oder Lücken im Histogramm sind oft der Ausgangspunkt für tiefere Analysen.

Kibana Query Language (KQL)

KQL ist die Abfragesprache in Kibana. Sie ist speziell für Analysten konzipiert.

Grundprinzip:

```
feldname: wert
```

Beispiel:

```
product.category: "Smartphones"
```

> KQL-Abfragen gibst du in die Suchleiste oben in Discover ein.

KQL - Freitextsuche

Ohne Feldnamen durchsuchst du alle Felder gleichzeitig:

```
Samsung Galaxy
```

Findet alle Dokumente, die "Samsung" **und** "Galaxy" in beliebigen Feldern enthalten.

Anführungszeichen für exakte Phrasen:

```
"Samsung Galaxy S24"
```

Findet nur Dokumente mit genau dieser Zeichenkette.

Abfrage	Ergebnis
`Samsung Galaxy`	Beide Wörter (beliebige Reihenfolge)
`"Samsung Galaxy"`	Exakte Phrase

KQL - Feld:Wert-Abfragen

Die präziseste Art zu suchen: Gib das Feld explizit an.

Abfrage	Beschreibung
`customer.city: "Berlin"`	Kunden aus Berlin
`product.category: "Laptops"`	Kategorie Laptops
`order.status: "shipped"`	Versendete Bestellungen
`customer.region: "Bayern"`	Kunden aus Bayern

Wichtig:

- Feldnamen sind case-sensitive
- Textwerte mit Leerzeichen in Anführungszeichen setzen
- Kibana bietet Autovervollständigung für Feldnamen und Werte

KQL - Vergleichsoperatoren

Für numerische Felder und Datumswerte stehen Vergleichsoperatoren zur Verfügung:

Operator	Bedeutung	Beispiel
`>`	Größer als	`order.total > 500`
`>=`	Größer oder gleich	`order.total >= 100`
`<`	Kleiner als	`order.total < 50`
`<=`	Kleiner oder gleich	`order.items_count <= 3`

Praxisbeispiel Mustertech GmbH:

Alle Bestellungen über 1000 Euro finden:

```
order.total > 1000
```

KQL - Boolesche Operatoren

Kombiniere Bedingungen mit `AND`, `OR` und `NOT`:

AND - beide Bedingungen müssen zutreffen:

```
product.category: "Laptops" AND order.total > 800
```

OR - mindestens eine Bedingung trifft zu:

```
customer.region: "Bayern" OR
  customer.region: "Baden-Württemberg"
```

NOT - Bedingung ausschließen:

```
order.status: "completed" AND
  NOT product.category: "Zubehör"
```

KQL - Klammern und Priorität

Verwende Klammern, um die Auswertungsreihenfolge festzulegen:

Ohne Klammern (mehrdeutig):

```
product.category: "Laptops" OR
  product.category: "Tablets" AND
  order.total > 500
```

Mit Klammern (eindeutig):

```
(product.category: "Laptops" OR
  product.category: "Tablets") AND
  order.total > 500
```

> Nutze immer Klammern, wenn du `AND` und `OR` in einer Abfrage kombinierst. So vermeidest du unerwartete Ergebnisse.

KQL - Wildcards

Das Sternchen `*` steht für beliebig viele Zeichen:

Abfrage	Findet
`product.name: Samsung*`	Samsung Galaxy, Samsung Tab, …
`customer.email: *@firma.de`	Alle Firmen-E-Mails
`product.sku: LPT-*`	Alle Laptop-Artikelnummern

Existenzprüfung - hat ein Feld überhaupt einen Wert?

```
customer.phone: *
```

Findet alle Dokumente, bei denen das Feld `customer.phone` vorhanden und nicht leer ist.

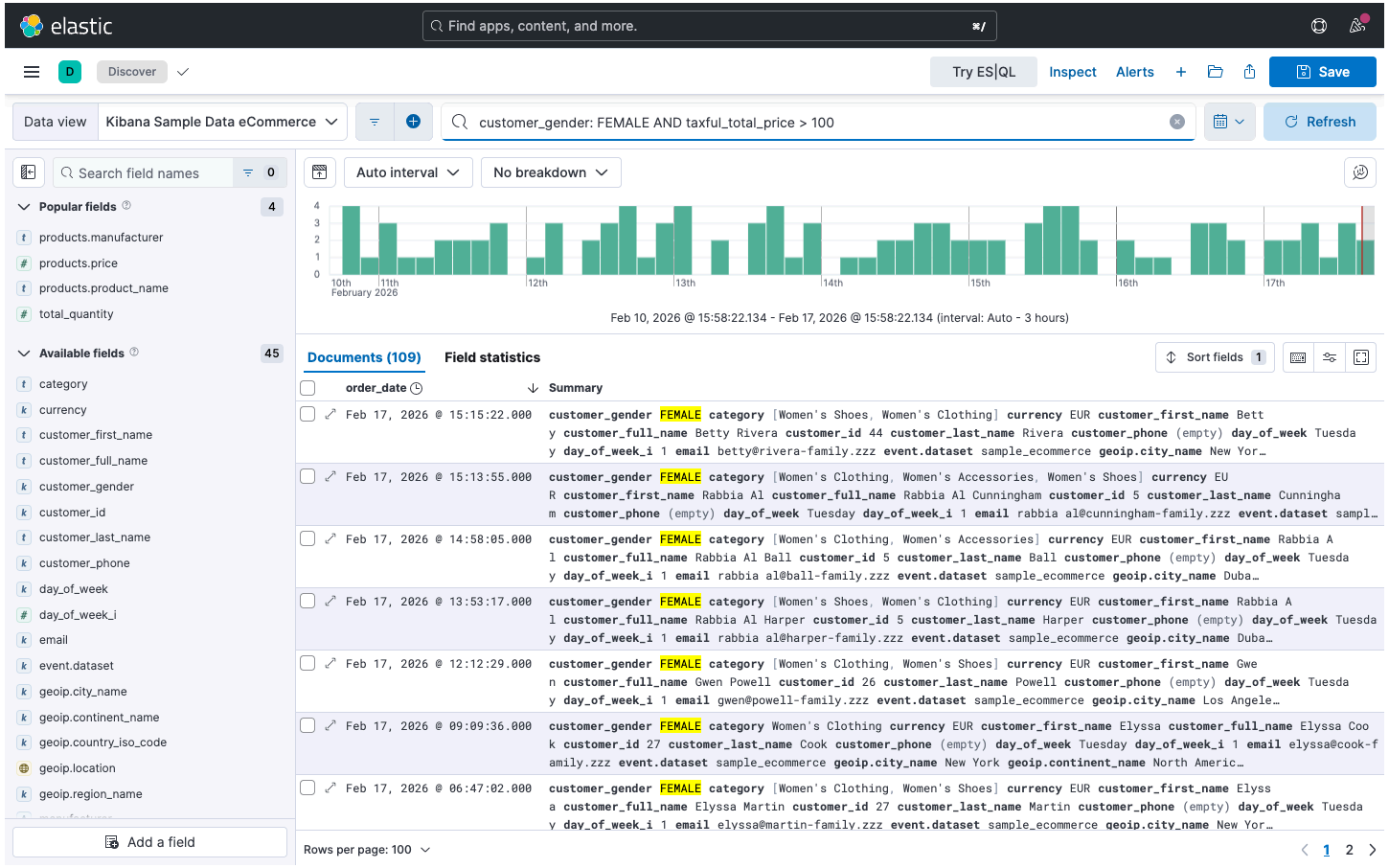
> Wildcards sind nützlich, können aber bei sehr großen Datenmengen langsam sein.

KQL - Übersicht der Syntax

Element	Syntax	Beispiel
Freitext	`text`	`Samsung`
Exakte Phrase	`"text"`	`"Samsung Galaxy"`
Feld:Wert	`feld: wert`	`customer.city: "Berlin"`
Größer als	`feld > wert`	`order.total > 500`
Kleiner als	`feld < wert`	`order.total < 50`
UND	`AND`	`a: 1 AND b: 2`
ODER	`OR`	`a: 1 OR a: 2`
NICHT	`NOT`	`NOT a: 1`
Wildcard	`*`	`name: Sam*`
Klammern	`()`	`(a: 1 OR a: 2) AND b: 3`
Existenz	`feld: *`	`phone: *`

KQL in Aktion

```
customer_gender: FEMALE AND taxful_total_price > 100
```



Filter verwenden

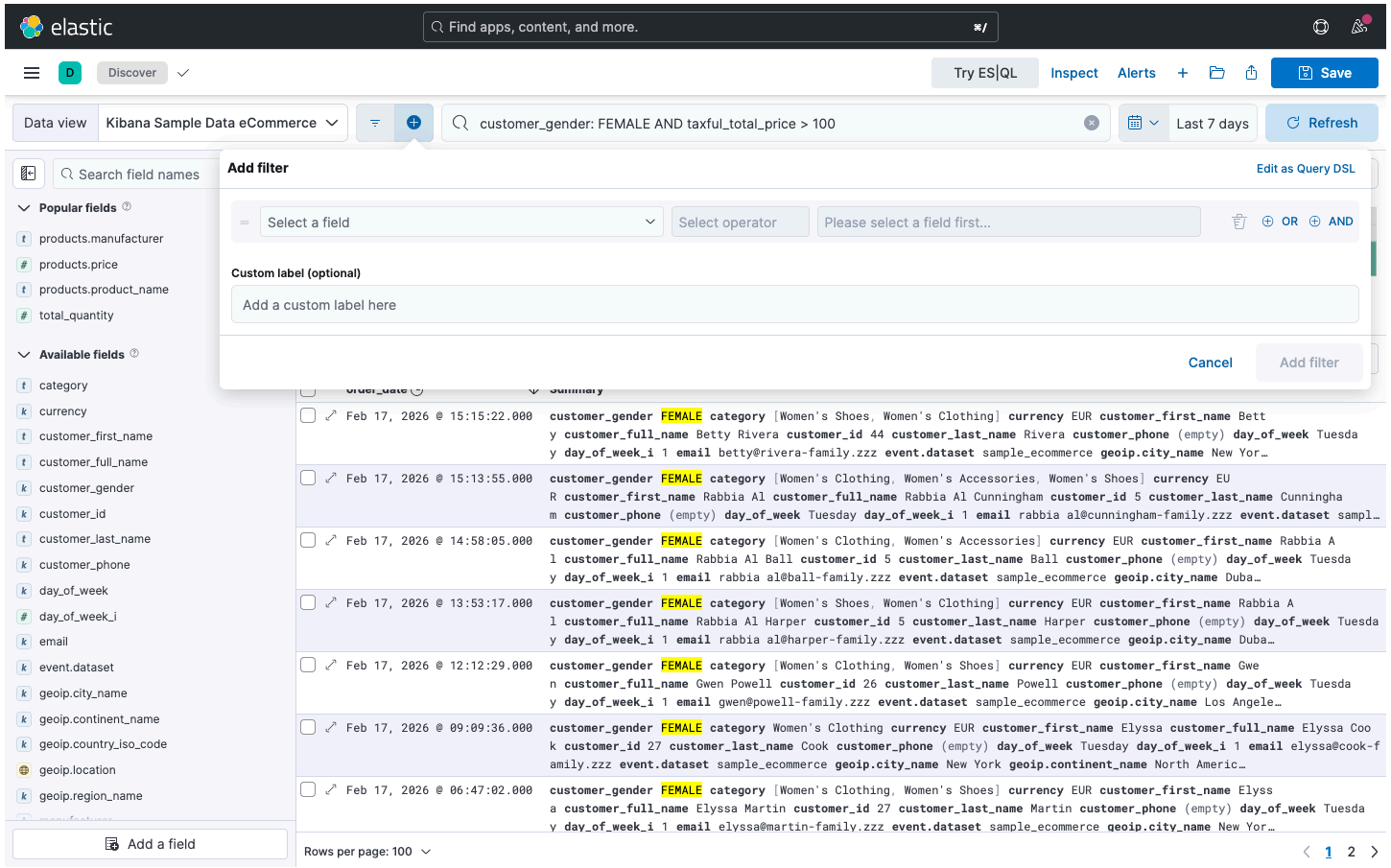
Neben KQL-Abfragen bietet Kibana eine
grafische Filter-Leiste unterhalb der Suchleiste.

Filter hinzufügen - drei Wege:

1. **Über die Felderliste:** Klicke auf ein Feld in der linken Seitenleiste und wähle einen Wert aus
2. **Über die Dokumententabelle:** Klicke auf ein Lupensymbol neben einem Feldwert
3. **Manuell:** Klicke auf "Add filter" in der Filter-Leiste

> Filter und KQL-Abfragen ergänzen sich. Nutze Filter für häufig wechselnde Bedingungen und KQL für komplexere Abfragen.

Filter hinzufügen - Dialog



Filter - Aktionen

Jeder aktive Filter bietet dir mehrere Aktionen per Klick:

Aktion	Beschreibung
Aktivieren/Deaktivieren	Filter temporär ein-/ausschalten
Pinnen	Filter bleibt beim Wechsel zwischen Tabs erhalten
Invertieren	Gegenteil anzeigen (z. B. alles außer "Laptops")
Bearbeiten	Filterbedingung nachträglich ändern
Löschen	Filter entfernen

Praxisbeispiel:

Du filterst auf `product.category: "Laptops"`. Durch Invertieren siehst du alle Bestellungen **ohne** Laptops.

Filter kombinieren

Mehrere Filter werden standardmäßig mit **AND** verknüpft.

Beispiel-Szenario bei Mustertech GmbH:

Du möchtest alle Laptop-Bestellungen aus Bayern mit einem Wert über 1000 Euro finden:

1. Filter: `product.category: "Laptops"`
2. Filter: `customer.region: "Bayern"`
3. KQL-Abfrage: `order.total > 1000`

Alle drei Bedingungen müssen gleichzeitig erfüllt sein.

> **Tipp:** Gepinnte Filter bleiben aktiv, auch wenn du zwischen verschiedenen Discover-Tabs oder Dashboards wechselst.

Spalten konfigurieren

In der Standardansicht zeigt Discover nur die Spalte `_source` mit dem gesamten Dokumentinhalt. Das ist unübersichtlich.

Spalten hinzufügen:

- Klicke in der Felderliste links auf das **Plus-Symbol** neben einem Feldnamen
- Oder klicke im aufgeklappten Dokument auf das Spaltensymbol neben einem Feld

Empfohlene Spalten für Bestellanalysen:

- `order.date`
- `customer.name`
- `product.category`
- `product.name`
- `order.total`

Spalten verwalten

Spalten neu anordnen:

- Ziehe Spaltenüberschriften per Drag & Drop an die gewünschte Position

Spalten entfernen:

- Klicke auf das X-Symbol in der Spaltenüberschrift

Spaltenbreite anpassen:

- Ziehe den Rand einer Spaltenüberschrift

Sortierung ändern:

- Klicke auf eine Spaltenüberschrift, um aufsteigend oder absteigend zu sortieren
- Mehrfachsortierung: Halte die Umschalttaste gedrückt

Dokumente im Detail untersuchen

Klicke auf einen Pfeil links neben einem Dokument, um es aufzuklappen.

Die Detailansicht zeigt:

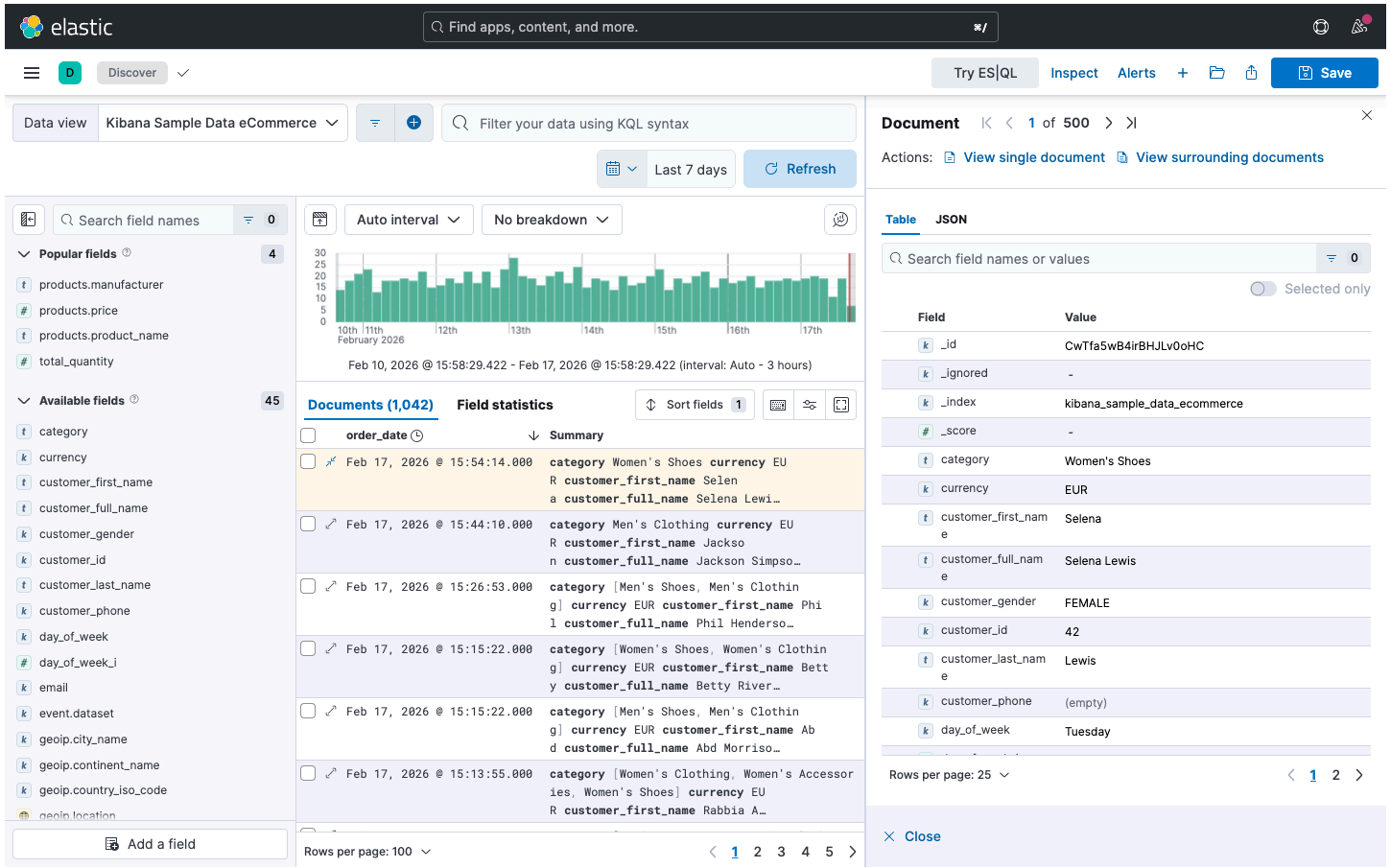
- **Tabelle:** Alle Felder mit Werten übersichtlich dargestellt
- **JSON:** Das Rohdokument im JSON-Format

Nützliche Aktionen in der Detailansicht:

- Feldwert als Filter hinzufügen (Plus-Symbol)
- Feldwert als Ausschlussfilter setzen (Minus-Symbol)
- Spalte zur Tabelle hinzufügen
- Feld in die Zwischenablage kopieren

> Die Detailansicht ist ideal, um einzelne Bestellungen genau zu prüfen.

Dokumente im Detail - Kibana



Verfügbare Felder - Die Seitenleiste

Die linke Seitenleiste zeigt alle verfügbaren Felder des aktuellen Data Views.

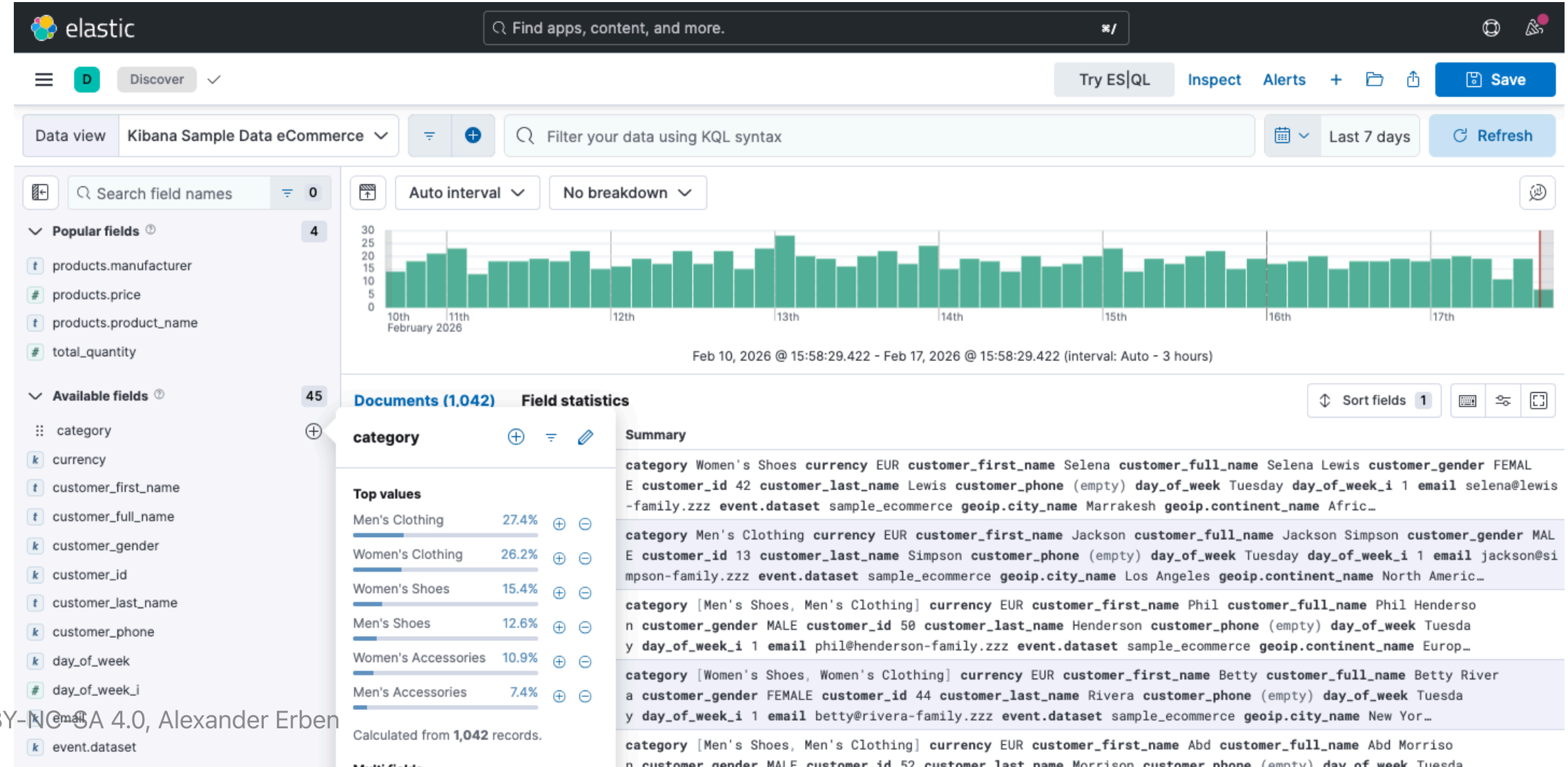
Feldtypen erkennen:

- **t** -- Textfeld (z. B. `customer.name`)
- **#** -- Numerisches Feld (z. B. `order.total`)
- **Kalender** -- Datumsfeld (z. B. `order.date`)
- **?** -- Boolean (z. B. `order.is_returned`)

Feldstatistiken:

Klicke auf ein Feld, um eine Schnellübersicht der häufigsten Werte zu sehen. So erkennst du z. B. sofort die beliebtesten Produktkategorien.

Verfügbare Felder - Feldstatistiken



Daten exportieren - CSV

Du kannst die aktuelle Trefferliste als CSV-Datei herunterladen:

1. Führe deine Suche mit Filtern und KQL durch
2. Klicke auf **Share** in der oberen Leiste
3. Wähle **CSV Reports** oder **Download CSV**
4. Warte, bis der Export erstellt ist
5. Lade die Datei herunter

Hinweise:

- Der Export enthält die aktuell sichtbaren Spalten
- Zeitfilter und Abfragen werden berücksichtigt
- Bei sehr großen Datenmengen kann der Export einige Zeit dauern
- Maximale Zeilenanzahl ist in Kibana konfigurierbar

Gespeicherte Suchen

Speichere häufig genutzte Abfragen, um sie schnell wiederzuverwenden:

Suche speichern:

1. Konfiguriere deine Abfrage, Filter und Spalten
2. Klicke auf **Save** in der oberen Leiste
3. Vergib einen aussagekräftigen Namen

Beispiele für sinnvolle Namen:

- "Laptop-Bestellungen Bayern > 1000 EUR"
- "Retouren letzte 30 Tage"
- "Bestellungen ohne Versandbestätigung"

> Gespeicherte Suchen können auch in Dashboards eingebettet werden - dazu mehr in Modul 03.

Zusammenfassung

Discover ist dein Einstiegspunkt für jede Datenanalyse in Kibana:

- **Zeitfilter** grenzen den Zeitraum ein - relativ für laufende Analysen, absolut für Berichte
- **KQL** bietet dir eine mächtige, aber einfache Abfragesprache mit Feld: Wert-Suche, Vergleichen, Wildcards und boolescher Logik
- **Filter** ergänzen KQL und lassen sich per Klick ein-/ausschalten, pinnen und invertieren
- **Spalten** konfigurierst du individuell für jede Analyse
- **Gespeicherte Suchen** und **CSV-Export** machen deine Ergebnisse nachhaltig nutzbar