



# Data Analysis with Kibana

An Elastic Training Course

[elastic.co/training](https://elastic.co/training)

8.8.1

# Welcome to Elastic virtual training

- The training will start with an audio/video test, to make sure that everyone can hear and see the instructors
- To prevent any audio/video issues, please:
  - use a supported web browser: Chrome or Firefox
  - open this page in an "incognito" or "private" window
  - disable any ad blockers, script blockers, proxy or VPN
- In case of problems, try the following steps in order:
  - click on the video panel in the top right to activate audio
  - refresh this web page
  - try another web browser
  - as a last resort, restarting your computer sometimes helps

# Welcome to Elastic training

- Visit **learn.elastic.co** and log in
  - follow instructions from registration email to get access
- Go to "**My Enrollments**" and click on today's training
- Download the PDF file from the "Content" tab
  - this contains all the slides and lab instructions
- Click on "**Access your virtual class here**" to access the Lab Environment

# About Elastic training

- Environment
  - Strigo test: <https://app.strigo.io/system-test>
- Introductions
- Code of Conduct
  - <https://www.elastic.co/community/codeofconduct>

# Data Analysis with Kibana: Agenda

- **Getting Started**

- Search your Data
- Visualize your Data
- Additional Visualizations
- Present your Data
- Analyze your Data with Machine Learning
- Advanced Kibana
- Alerting

# Getting Started

Module 1

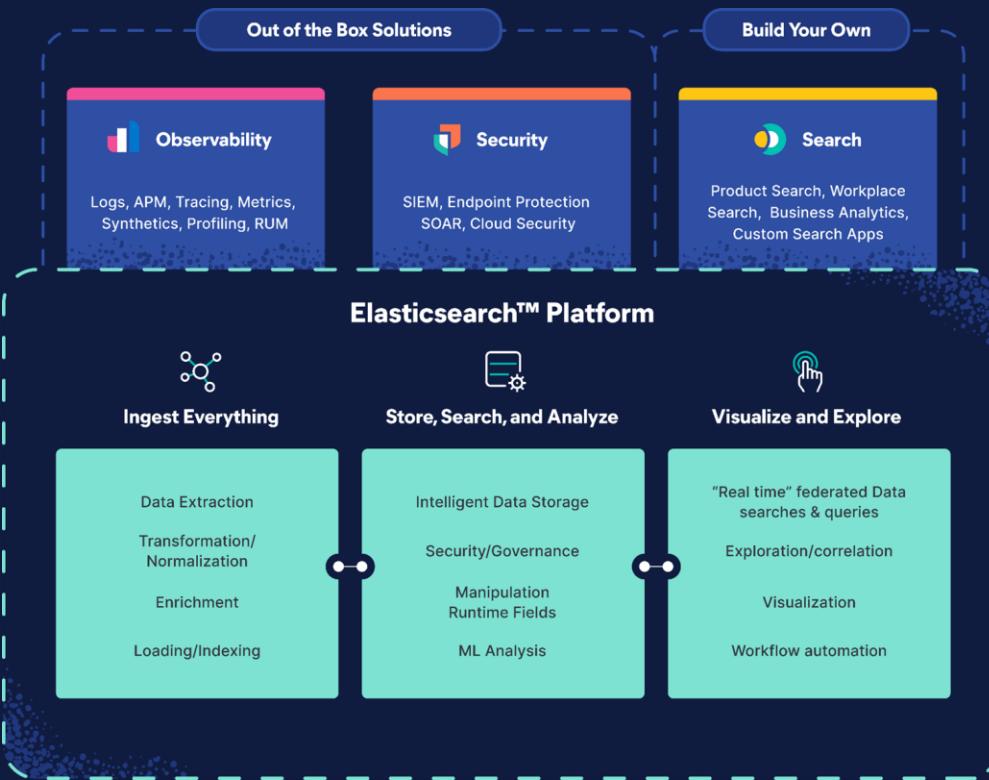
# Lessons

- Introduction to the Kibana
- Hello, Dashboard!
- Your Space

# Introduction to Kibana

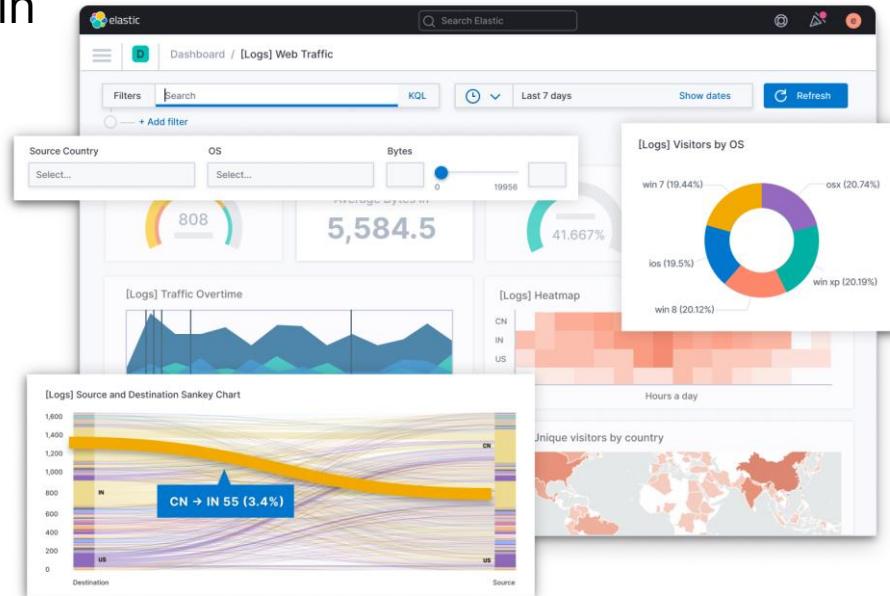
Module 1 Lesson 1

# The Elastic Search Platform

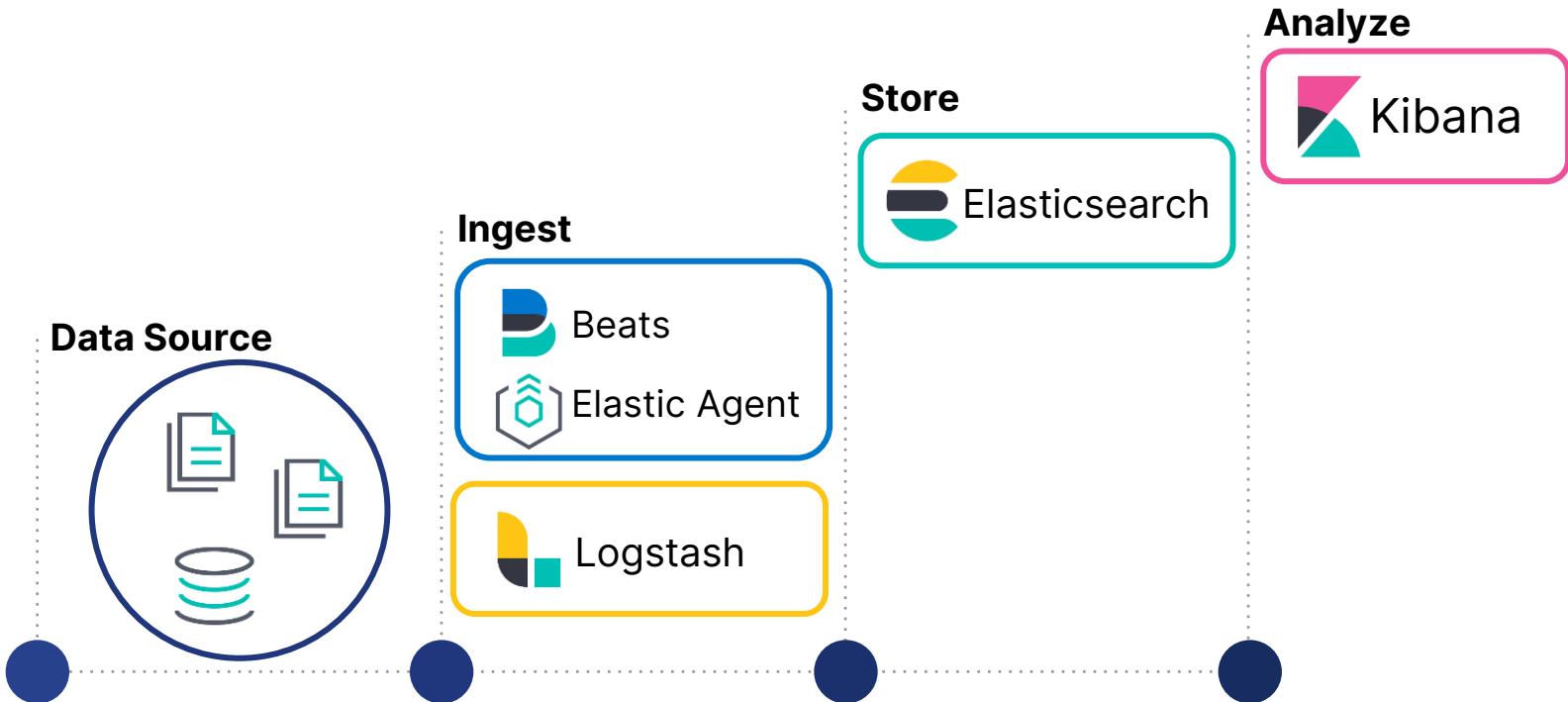


# Kibana

- Kibana is the window into the Elastic Stack
- UI layer
- for visualizing and exploring data in Elasticsearch
- for managing the Elastic Stack

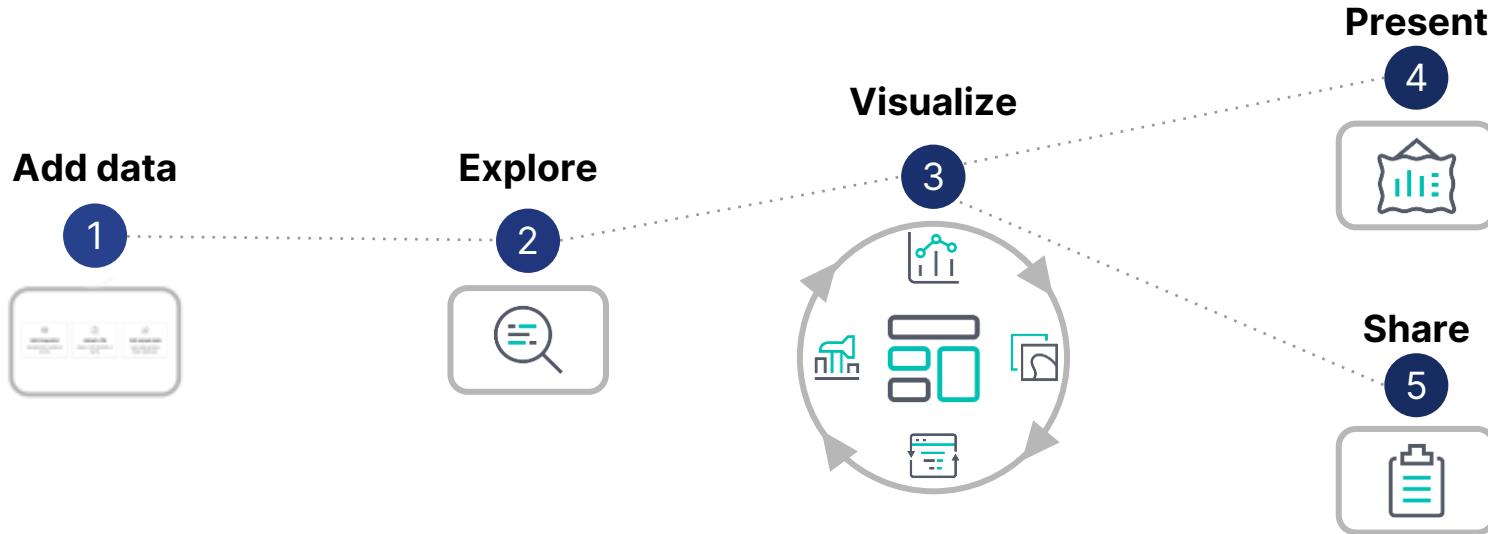


# Elasticsearch data journey



# Visualize and Analyze

Data analysis is a core functionality of Kibana



# Kibana Home Page

- Provides access to the solutions, and everything you need to visualize and analyze your data

The screenshot shows the Kibana Home Page with a dark header bar featuring the elastic logo, a search bar, and user icons. Below the header, a navigation bar includes a menu icon, a 'D' icon, and a 'Home' button. The main content area has a light gray background and displays four cards:

- Enterprise Search**: A yellow card with a white circular icon containing a stylized 'E'. Description: "Create search experiences with a refined set of APIs and tools."
- Observability**: A pink card with a white circular icon containing a bar chart. Description: "Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs."
- Security**: A teal card with a white circular icon containing a shield-like shape. Description: "Prevent, collect, detect, and respond to threats for unified protection across your infrastructure."
- Analytics**: A blue card with a white circular icon containing a stylized 'K'. Description: "Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications."

# Add data

- Collect your data
- Upload a file that contains your data
- Add a sample data set

[Try sample data](#)

## Add data

All Logs Metrics Security [Sample data](#) [Upload file](#)

[Try Integrations](#)

### INSTALLED

**Sample eCommerce Data**  
This dashboard contains sample data for you to play with. You can use it to experiment with different visualizations and search queries.  
View data

**Sample flight data**  
This dashboard contains sample flight data for you to play with. You can use it to experiment with different visualizations and search queries.  
View data

**Sample web logs**  
This dashboard contains sample web log data for you to play with. You can use it to experiment with different visualizations and search queries.  
View data

### Sample eCommerce orders

Sample data, visualizations, and dashboards for tracking eCommerce orders.

[Remove](#) [View data](#)

### Sample flight data

Sample data, visualizations, and dashboards for monitoring flight routes.

[Remove](#) [View data](#)

### Sample web logs

Sample data, visualizations, and dashboards for monitoring web logs.

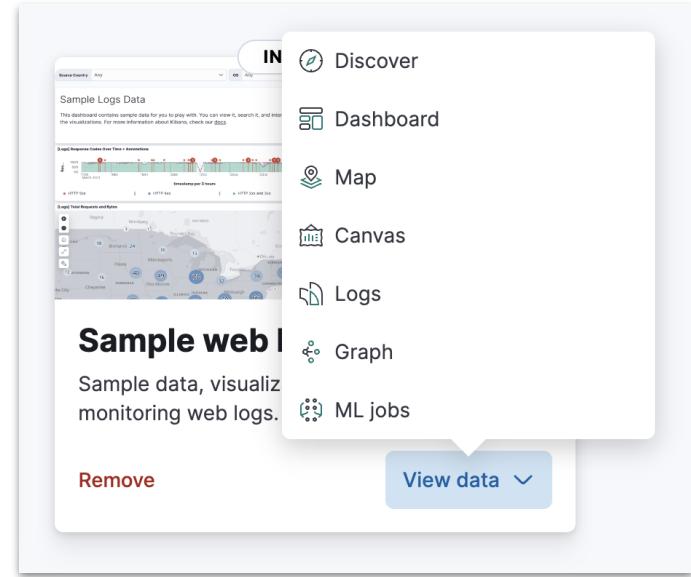
[Remove](#) [View data](#)

Examples in slides use eCommerce data

Labs use web log data

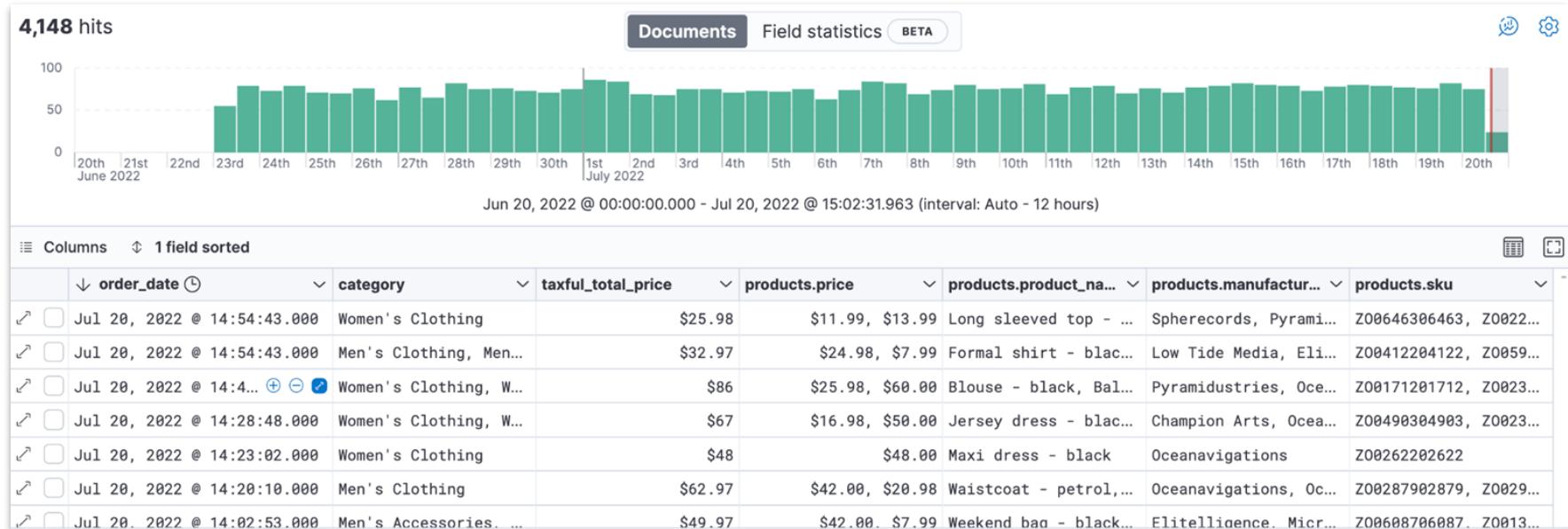
# Sample data

- Kibana sample data integration contains
  - Data set
  - Dashboards
  - Visualizations
  - Canvas workpads
  - Preconfigured ML jobs



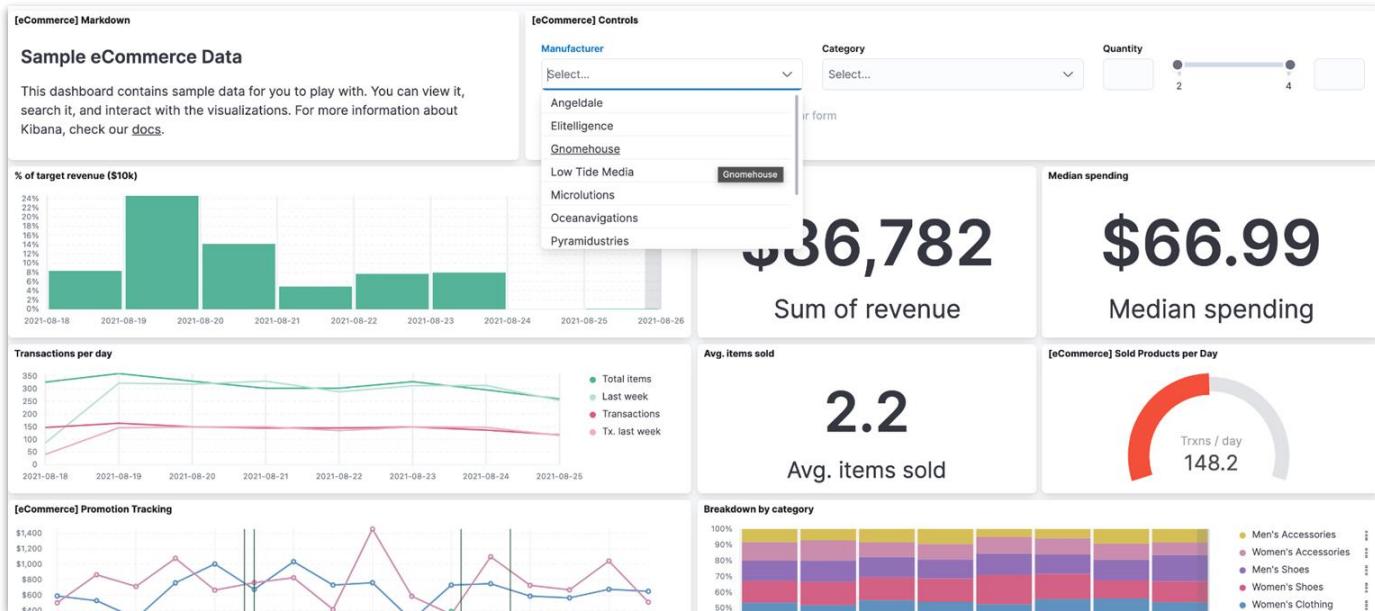
# Explore

- Use Discover to search your data for hidden insights and relationships



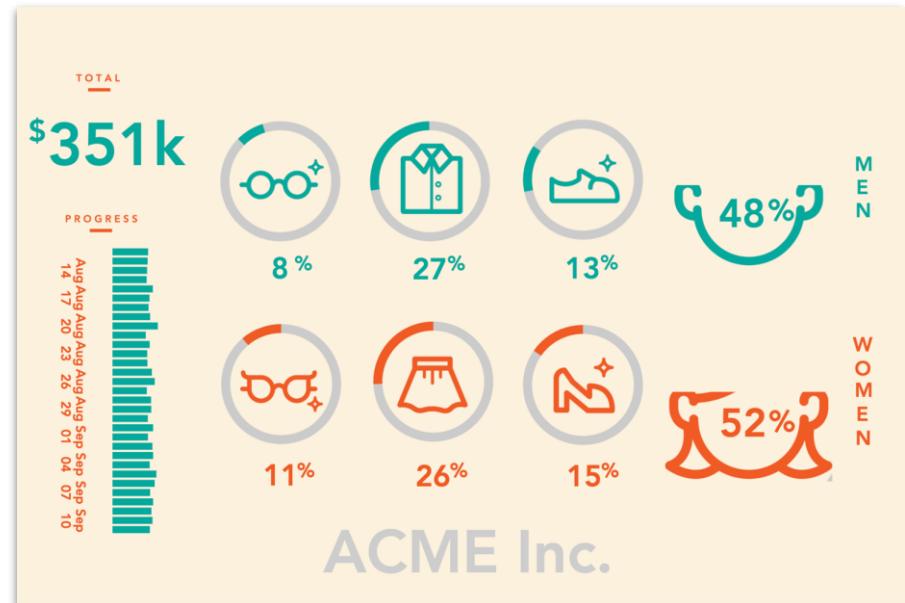
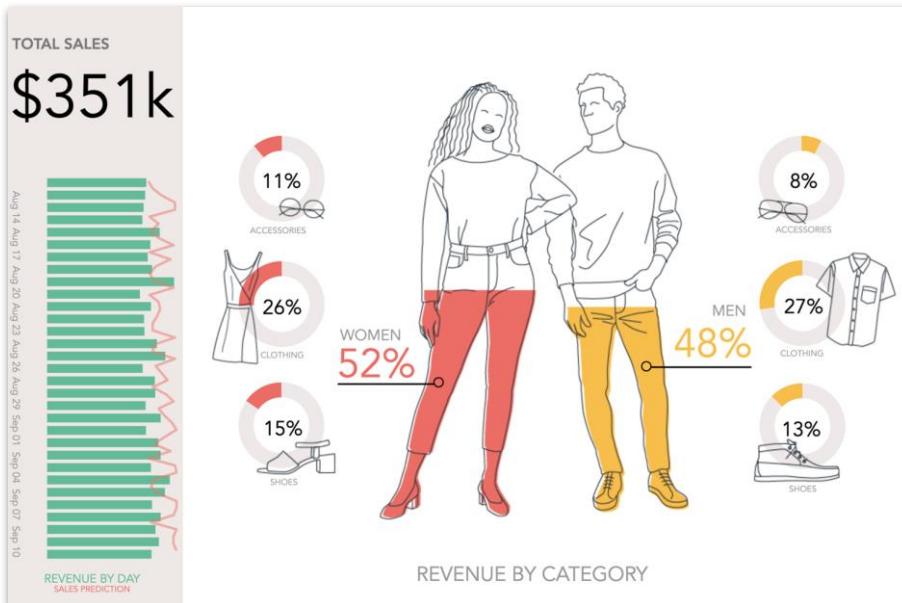
# Visualize

- Dashboard is your starting point to create visualizations
- Visualize to tell a story about your data



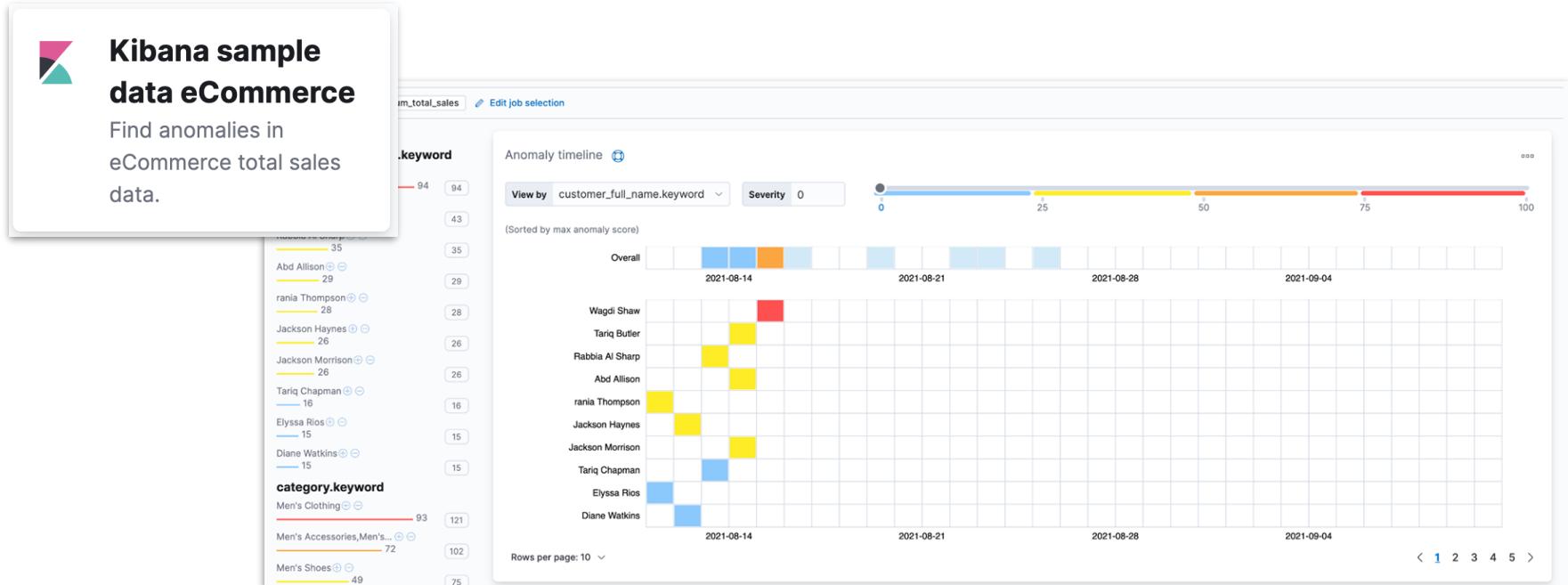
# Present

- Display your data on a visually compelling, pixel-perfect workpad with Canvas



# Model data behavior

- Extract insights from your data that you might otherwise miss



# Get notifications

- Create alerts to trigger actions when conditions are met
  - detect complex conditions
  - trigger actions with built-in connectors
- Integrated with
  - Observability
  - Security Maps
  - Machine Learning

Create rule

Name: Kibana sites - high egress

Tags (optional):

**Index threshold**  
Alert when an aggregated query meets the threshold. [Learn more](#)

Select an index:  
INDEX kibana\_sample\_data\_logs  
WHEN sum()  
OF bytes  
GROUPED OVER top 4 'host.keyword'

Define the condition:  
IS ABOVE 42000

Cancel Save

**Actions**  
Select a connector type

Connector Type	Icon	Connector Name
Email	envelope	IBM Resilient
Index	document	Jira
Opsgenie	person	Microsoft Teams
PagerDuty	P	ServiceNow ITOM
Server log	log	ServiceNow ITSM
ServiceNow SecOps	now	Torq
Slack	S	Webhook
Swimlane	swimlane	xMatters

# Summary: Introduction to Kibana

Module 1 Lesson 1

# Summary

- Elasticsearch, Kibana, Logstash, Beats, and Elastic Agent integrations are components of the Elastic Stack
- Kibana can be used to manage the Elastic Stack
- Kibana can be used to add, explore, visualize, present, and share your data

# Quiz

- 1. True or False:** Kibana is known as your window into Elastic Stack.
- 2. True or False:** Kibana can be used to manage Elasticsearch clusters.
- 3. True or False:** Data is stored in Kibana.

# Introduction to Kibana

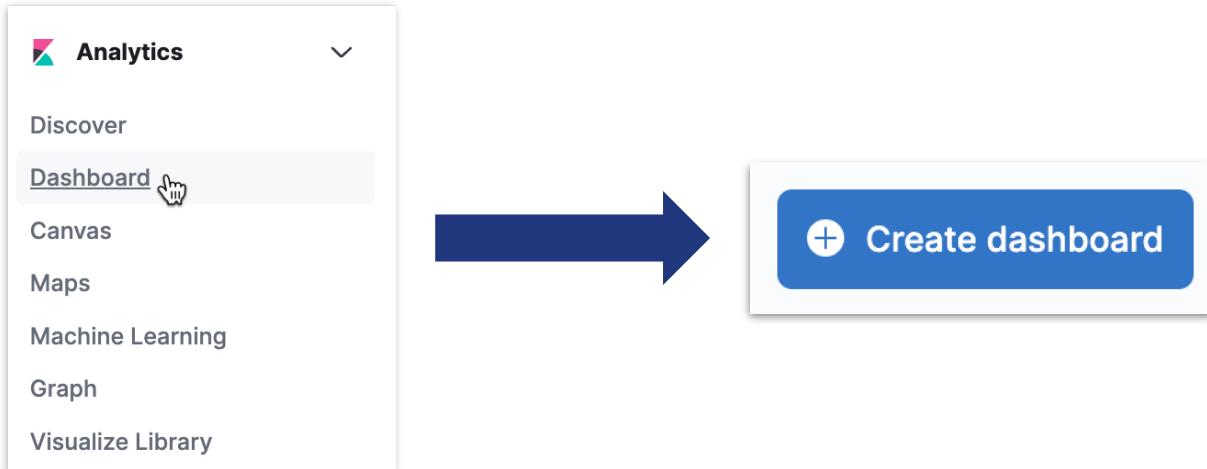
Lab 1.1 - Load sample data

# Hello, Dashboard!

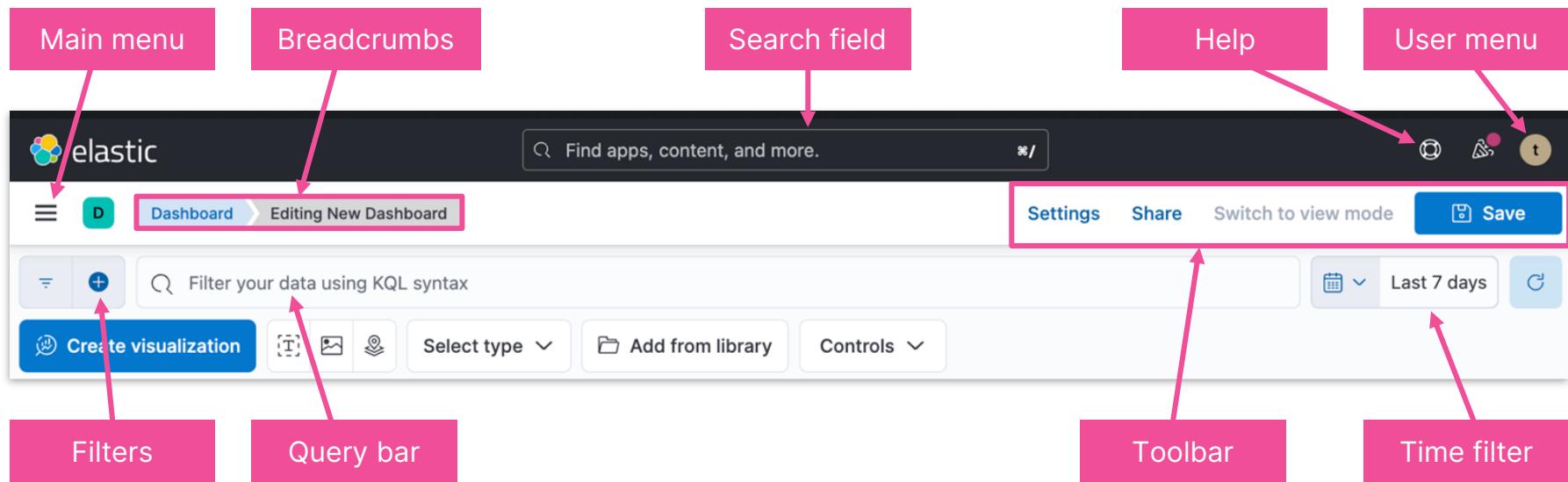
Module 1 Lesson 2

# Build your first dashboard

- Sample dashboards are great for:
  - exploring what's possible in visualizations
  - learning how to build visualizations
- When you're ready, build your own dashboard

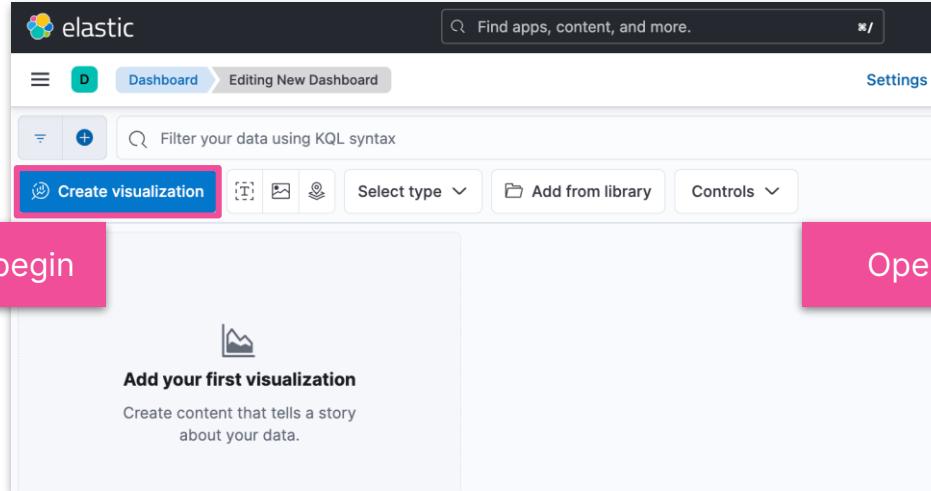


# Get to know the interface



# Visualization editor

- Kibana provides several editors that you can use to visualize your data
- Each editor supports different features



Opens Lens visualization editor

# Lens interface

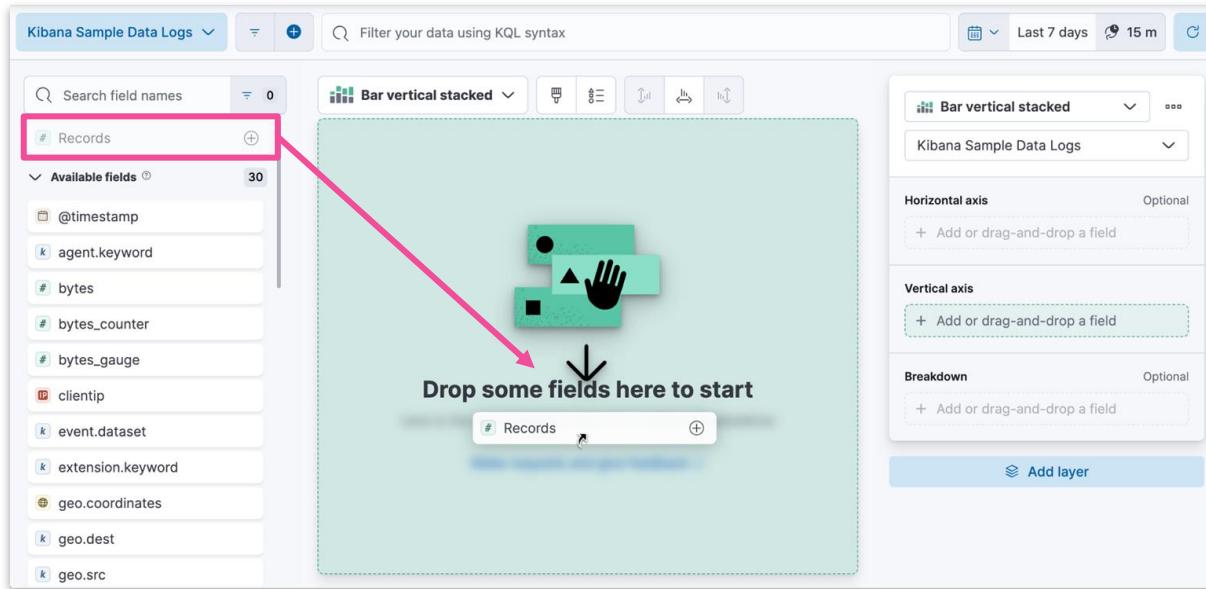
The image shows the Kibana Lens interface with four main sections highlighted by pink boxes:

- Data view**: Shows the search bar "Kibana Sample Data eCommerce", a search field "Search field names", and a list of "Available fields" including "category.keyword", "currency", "customer\_birth\_date", "customer\_first\_name.keyword", "customer\_full\_name.keyword", "customer\_gender", "customer\_id", "customer\_last\_name.keyword", "customer\_phone", "day\_of\_week", "day\_of\_week\_i", "email", and "event.dataset".
- Fields list**: Shows a visualization type "Bar vertical stacked" and a search bar "Filter your data using KQL syntax".
- Workspace**: Shows a central area with a placeholder message "Drop some fields here to start" and a hand icon.
- Layer pane**: Shows settings for "Horizontal axis", "Vertical axis", and "Breakdown", each with an "Optional" label and a "+ Add or drag-and-drop a field" button. It also features an "Add layer" button.

Arrows point from the labels to their respective sections in the interface. A central graphic features a hand icon with arrows pointing towards the workspace area.

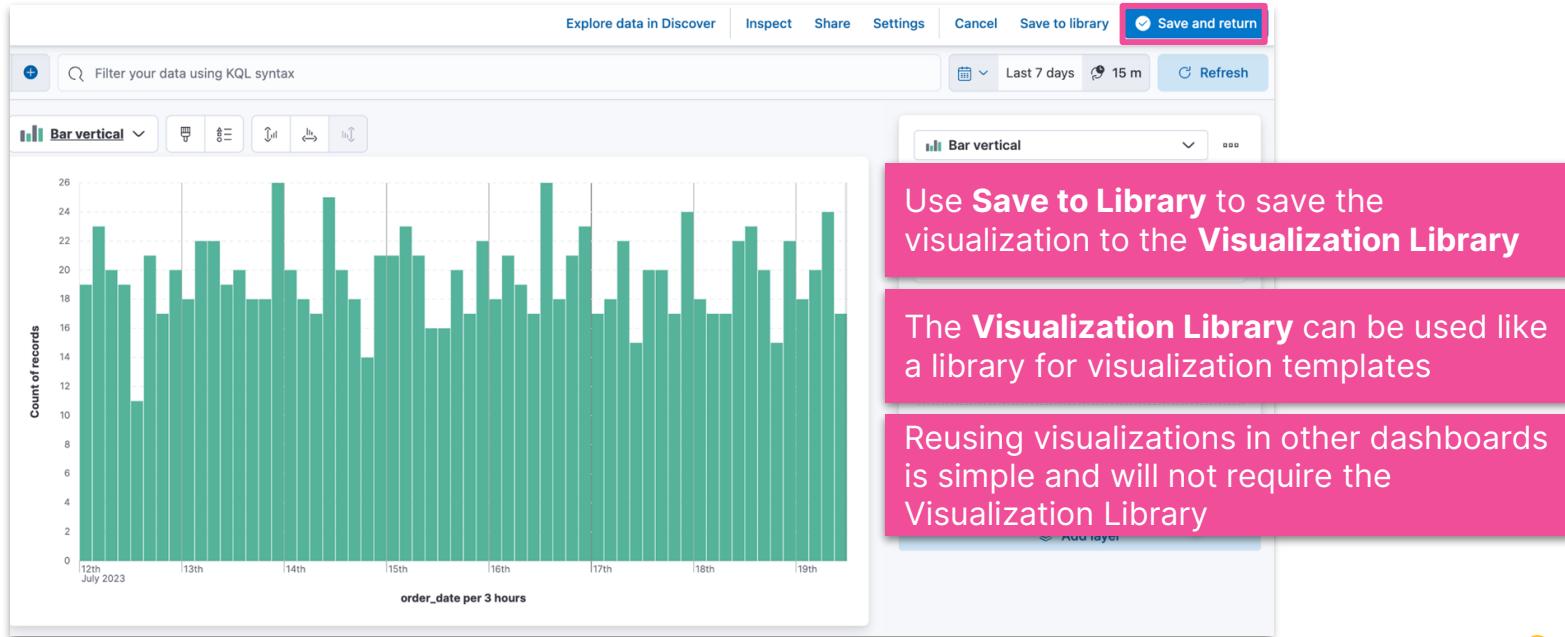
# Build your first visualization

- Select the correct **Data view** and **Time filter** range
- Just drag and drop a field from the fields list to the workspace



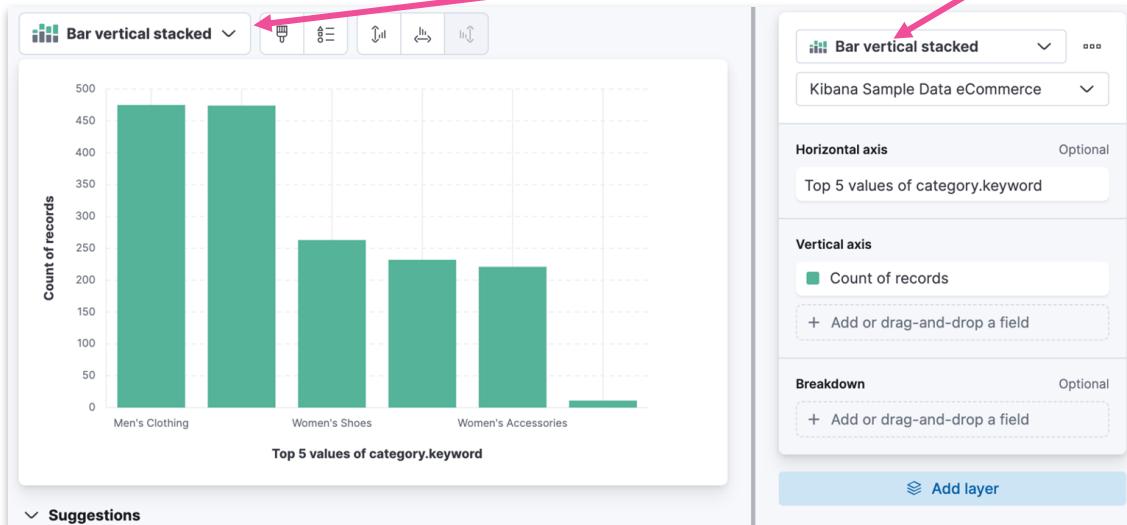
# Save to dashboard

- Click **Save and return** to go back to the dashboard
  - Your new Lens visualization is a new panel on your dashboard



# Add more panels

- Click **Create visualization** to return to Lens
- Explore different visualization types



Kibana guessed that you might want to see **Bar vertical stacked** for the category field

Kibana also guessed that you might want to see the **count** of the **top values** of category

# Change visualization type

- Choose from many different visualizations

The screenshot shows a user interface for creating and changing visualizations. At the top, there is a blue button labeled "Create visualization" and several icons for text, image, and file operations. To the right of these are "Select type" and "Add from library" dropdowns, and "Controls" settings.

The main area features a pie chart with the following data:

Category	Percentage
Men's Clothing	30.46%
Women's Clothing	28.05%
Women's Shoes	15.54%
Men's Shoes	13.99%
Women's Accessories	11.52%
Other	0.43%

A large blue arrow points from the pie chart towards a sidebar titled "Visualization type". This sidebar lists various visualization options categorized into Tabular, Bar, Line and area, Magnitude, Map, Proportion, and Technical preview.

**Tabular**

- Table

**Bar**

- Bar horizontal
- Bar horizontal percentage
- Bar horizontal stacked
- Bar vertical
- Bar vertical percentage
- Bar vertical stacked

**Line and area**

- Area
- Area percentage
- Area stacked
- Line

**Magnitude**

- Heat map

**Map**

- Region map

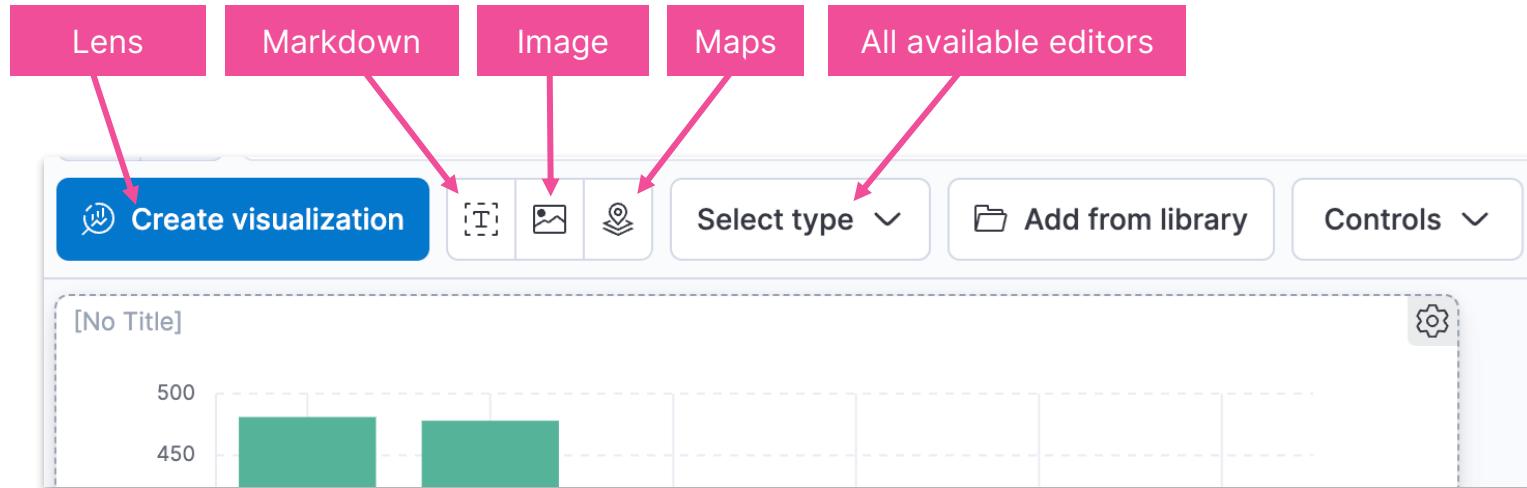
**Technical preview**

**Proportion**

- Donut
- Mosaic
- Pie
- Treemap
- Waffle

# Add more panels

- There are also other editors available
  - legacy editors located under **Select type -> Aggregation based**



# Add a description

- Use the **Text** editor to add text to your dashboard

The screenshot shows the Kibana Text editor interface. On the left, there's a preview area with the following content:

```
# Hello, Dashboard!
## This is my first dashboard.
it uses the **eCommerce sample dataset.

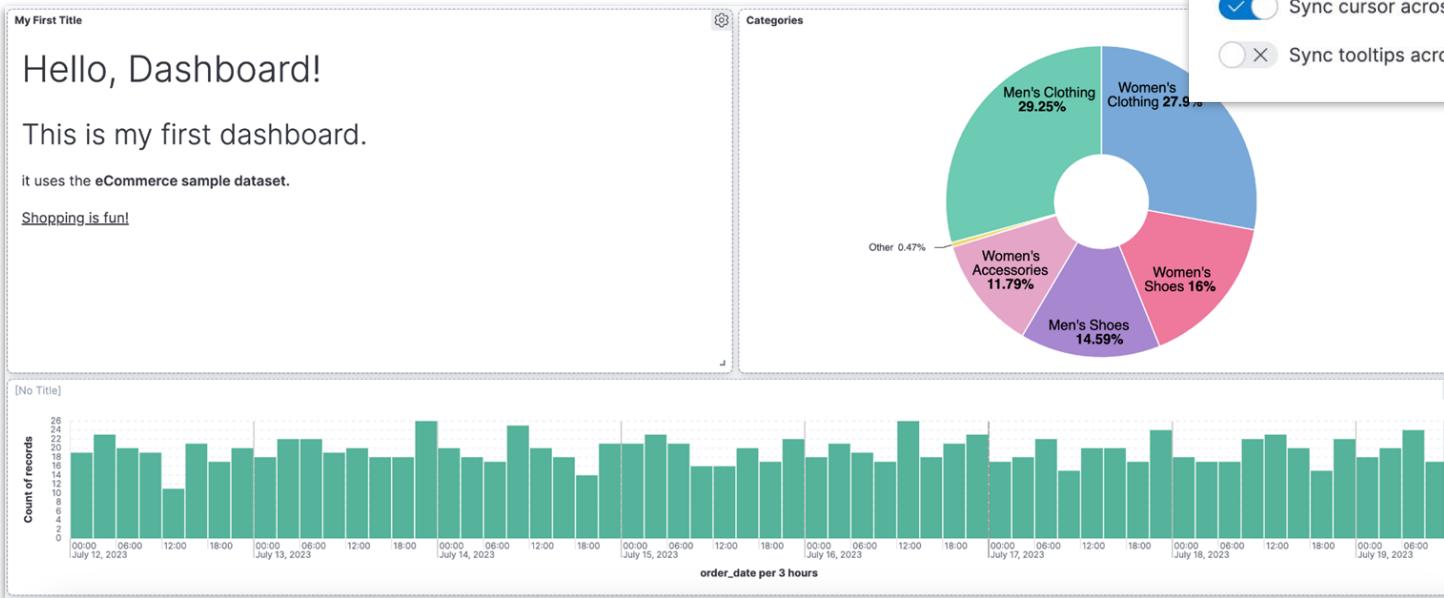
Shopping is fun!
```

A pink callout box highlights the text "Kibana's **Text** editor uses a GitHub-flavored markdown syntax".

On the right, the editor interface has tabs for "Data" and "Options". The "Data" tab is selected, showing the "Markdown" section with the same content. There's a "Help" link and a pink callout box with the text "Click Help for more info". At the bottom, there are buttons for "Discard", "Update", and a status indicator "Off".

# Rearrange your dashboard

- Panels can be moved and resized
- Panel titles can be added or removed



## Settings

- Use margins between panels
- Show panel titles
- Sync across panels**
  - Sync color palettes across panels
  - Sync cursor across panels
  - Sync tooltips across panels

# Save your dashboard

- Save your dashboard
  - **Switch to view mode** will become available
  - Click **Edit** to return to edit mode

Enable Store time with dashboard  
to set a default time range  
for your dashboard

## Save dashboard

### Title

Hello, Dashboard!

### Description

My first dashboard

### Tags

Store time with dashboard

This changes the time filter to the currently selected time each time this dashboard is loaded.

Cancel

Save

# Dashboard options for visualizations

- **Save to library:** saves the visualization to the Visualization Library
- **Copy to dashboard:** copies the visualization to a new or existing dashboard



# Summary: Hello, Dashboard!

Module 1 Lesson 2

# Summary

- Go to **Dashboard** to begin building visualizations
- Use **Lens** to build visualizations easily
- Select from many chart types
- Use the **Text** editor to add text to your dashboard
- Rearrange the panels on your dashboard in edit mode

# Quiz

- 1. True or False:** Dashboards are used to turn your data into a collection of panels containing visualizations
2. What is the name of the recommended editor to build visualizations for your dashboard?
- 3. True or False:** Visualizations can be copied between different dashboards

# Hello, Dashboard!

Lab 1.2 - Create your first dashboard

# Your Space

Module 1 Lesson 3

# Spaces

- Spaces enable you to organize your dashboards and other saved objects into meaningful categories

The image shows a screenshot of the Elasticsearch interface. At the top, there's a pink callout box with white text that reads: "You can even define the home page of your space". Below this, there are two main sections. The first section, labeled "Welcome home", contains four cards: "Enterprise Search" (yellow), "Observability" (pink), "Security" (teal), and "Analytics" (blue). Each card has a small icon and a brief description. The second section, labeled "Analytics", also contains a card with the same "Analytics" icon and description. The overall layout is clean and organized, demonstrating how spaces can be used to group related features.

You can even define the home page of your space

Welcome home

Enterprise Search

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

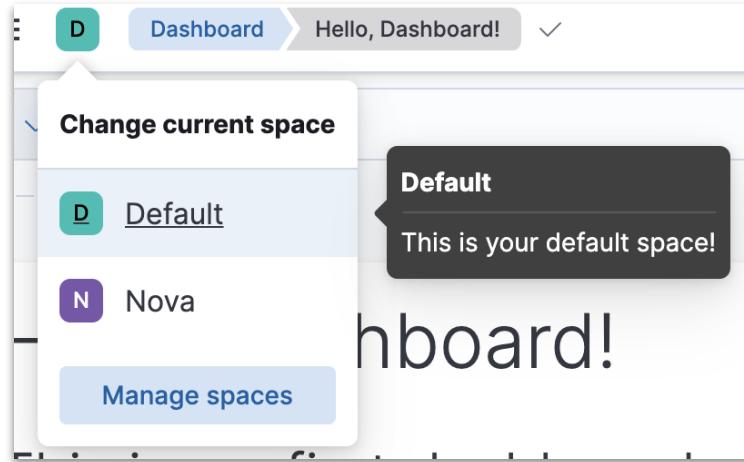
Welcome home

Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

# Default Space

- Kibana creates a default space for you
  - It's called **Default**



# Create a Space

- Go to the Space Manager from
  - Spaces menu -> Manage spaces
  - Main menu -> Stack Management -> Spaces

## Edit space

Organize your dashboards and other saved objects into meaningful categories.

### General

**Describe this space**  
Give your space a name that's memorable.

**Name**  
Nova

**Description**  
The new space

Optional

The description appears on the space selection screen.

Create a new space called **Nova**

# Edit your Space

- Select which Kibana features can be accessed in your new space

**Features**

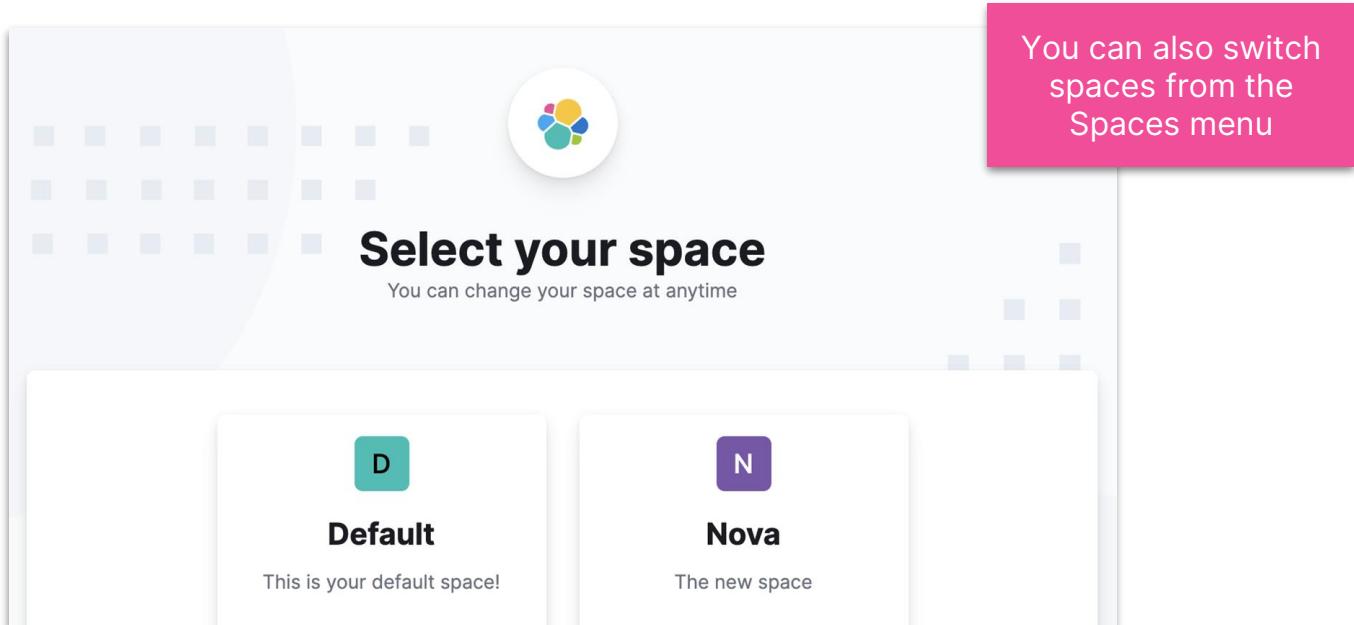
**Set feature visibility**

Hidden features are removed from the user interface, but not disabled. To secure access to features, [manage security roles](#).

Feature visibility	Show all	Hide all
<input checked="" type="checkbox"/>  <b>Analytics</b>	7/7 features visible	
<input checked="" type="checkbox"/>  Discover		
<input checked="" type="checkbox"/>  Dashboard		
<input checked="" type="checkbox"/>  Canvas		
<input checked="" type="checkbox"/>  Maps		
<input checked="" type="checkbox"/>  Machine Learning		
<input checked="" type="checkbox"/>  Graph		
<input checked="" type="checkbox"/>  Visualize Library		
<input type="checkbox"/>  Enterprise Search		
<input type="checkbox"/>  Observability	0/6 features visible	
<input type="checkbox"/>  Security	0/2 features visible	
<input checked="" type="checkbox"/>  Management	17/17 features visible	

# Select your Space

- Once a new space is created, you will be asked to select a space when you log in to Kibana



# Where's my dashboard!?

- Your new space will be empty!
  - your dashboard and all the sample objects are stored in the **Default** space
- If you go to Dashboard you will be asked to create a data view

You have data in Elasticsearch.  
Now, create a data view.

Data views identify the Elasticsearch data you want to explore. You can point data views to one or more data streams, indices, and index aliases, such as your log data from yesterday, or all indices that contain your log data.

[+ Create data view](#)



# Scope of a Space

- Your data set is still accessible from your space
  - but all the Kibana objects stored to access that data exists only in the Default space
- Kibana requires a data view to access the Elasticsearch data that you want to explore
  - a data view can point to one or more indices, data stream, or index aliases
  - for example, a data view can point to your log data from yesterday, or all indices that contain your data

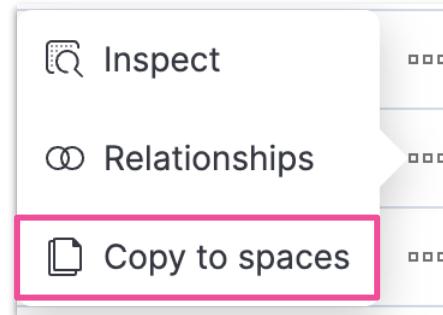
# Data view

- You can create a new data view
  - or copy over an existing data view from another space

**Saved Objects**

Manage and share your saved objects. To edit the under to its associated application.

Search...  
Type Title  
 [Logs] Web Traffic  
 [Flights] Overview  
 [eCommerce] Revenue Tracking  
 Advanced Settings [7.15.0-SNAPSHOT]  
 [Logs] Web Traffic  
 [eCommerce] Revenue Dashboard  
 [Flights] Global Flight Dashboard  
 Hello, Dashboard!  
 Kibana Sample Data - Data Logs



**Copy to spaces**

Hello, Dashboard!

**Copy options**

Create new objects with random IDs  
 Check for existing objects  
 Automatically overwrite conflicts  
 Request action on conflict

**Relationship**

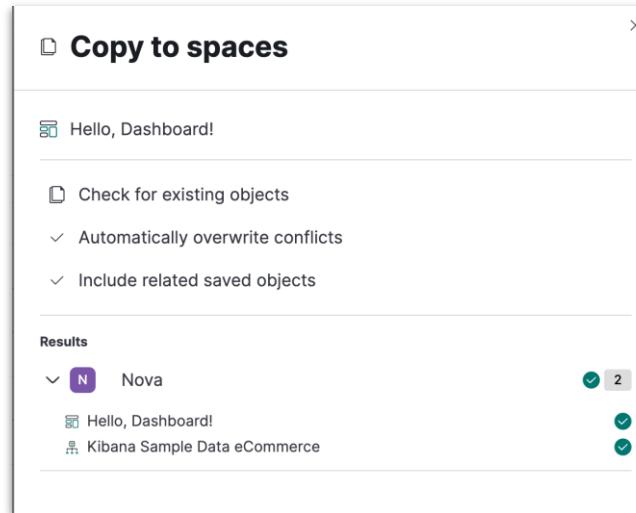
Include related objects

**Select spaces**

Nova

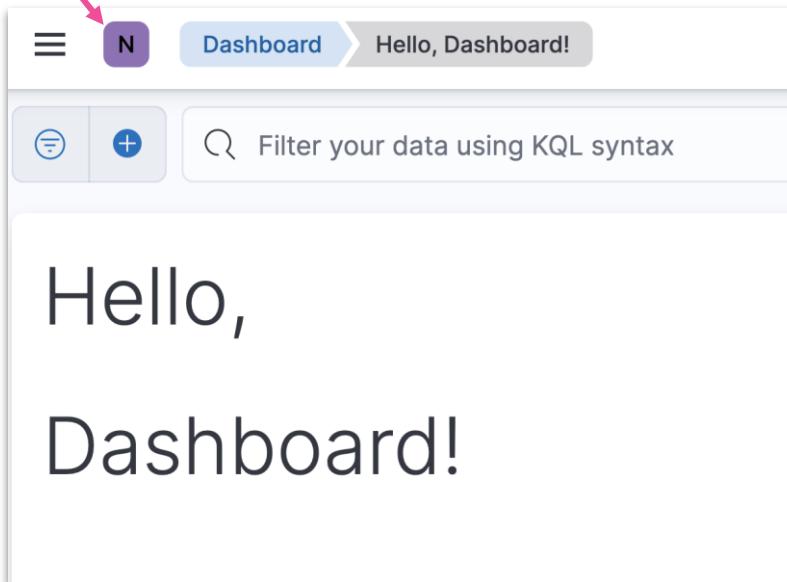
# Related Objects

- Kibana knows which objects have relationships to other objects
  - for example, the **Hello, Dashboard!** dashboard uses the **Kibana Sample Data eCommerce** data view
- Use **copy to spaces** to copy all related objects to a space



# Check out your new space

Avatar for  
your Space



Kibana objects created in the  
**Nova** space will not appear in the  
**Default** space

The **Saved Objects** page in  
the **Nova** space will now look  
very different from  
the **Saved Objects** page in  
the **Default** space

# Summary: Your Space

Module 1 Lesson 3

# Summary

- **Spaces** can be used to organize dashboards, visualizations and other Kibana objects
- You can easily copy Kibana objects from one space to another from **Saved Objects**

# Quiz

- 1. True or False:** Kibana creates a default space called “Default”
2. How can you separate the workspace for users who are working with the same dataset?
3. How do you share dashboards between spaces?

# Your Space

Lab 1.3 - Create a new space “Nova” and copy over your dashboard to Nova

# Data Analysis with Kibana: Agenda

- Getting Started
- **Search your Data**
- Visualize your Data
- Additional Visualizations
- Present your Data
- Analyze your Data with Machine Learning
- Advanced Kibana
- Alerting

# Search your Data

Module 2

# Lessons

- Discover and Data Visualizer
- KQL and Filters
- Field Focus

# Discover and Data Visualizer

Module 2 Lesson 1

# Documents

- In the Elastic Stack, data is stored in Elasticsearch indices
  - Elasticsearch is a **document store**
  - it stores data as JSON objects, called documents
  - Kibana **data view** specifies which Elasticsearch data you want to access

```
2017/02/14 5:42:14 Python Ghost Rider
1 Caused by: java.lang.ExceptionInInitializerError
2 at org.elasticsearch.common.logging.ESLogger.<clinit>(ESLogger.java:26)
3 at org.elasticsearch.search.common.xcontent.XContentRegistry.<clinit>(XContentRegistry.java:26)
4 at org.elasticsearch.common.xcontent.XContentRegistry.<clinit>(XContentRegistry.java:26)
5 at org.elasticsearch.common.settings.Settings.<clinit>(Settings.java:26)
6 at org.elasticsearch.common.settings.Settings.<clinit>(Settings.java:26)
7 at org.elasticsearch.common.settings.Settings.<clinit>(Settings.java:26)
8 at org.elasticsearch.common.settings.Settings.<clinit>(Settings.java:26)
9 at org.elasticsearch.common.settings.Settings.<clinit>(Settings.java:26)
10 at org.elasticsearch.common.network.NetworkModule.<clinit>(NetworkModule.java:26)
11 at org.elasticsearch.common.transport.TransportClient.<clinit>(TransportClient.java:26)
12 at org.elasticsearch.client.Client.<clinit>(Client.java:26)
13 at org.elasticsearch.client.transport.TransportClient.<init>(TransportClient.java:268)
14 at org.elasticsearch.transport.client.PreBuiltTransportClient.<init>(PreBuiltTransportClient.java:125)
15 at org.elasticsearch.transport.client.PreBuiltTransportClient.<init>(PreBuiltTransportClient.java:111)
16 at org.elasticsearch.transport.client.PreBuiltTransportClient.<init>(PreBuiltTransportClient.java:101)
17 at com.relicomgroup.bpo.reruse.util.TransportClientFactory.configureClients(TransportClientFactory.java:81)
```



# Fields and values

- Documents have **fields**
- Every field:
  - can have 0 or more **values**
  - has a **data type**



# Elasticsearch data types

- **Numeric** #

- Long
- Double

- **Text** t

- **Keyword** k

- **Date** 📅

- Date
- Date nanos

- **Boolean** 🎨

- **Geo types** 🌎

- **IP** IP

- **Range**

- Date
- IP
- Numeric

- ...

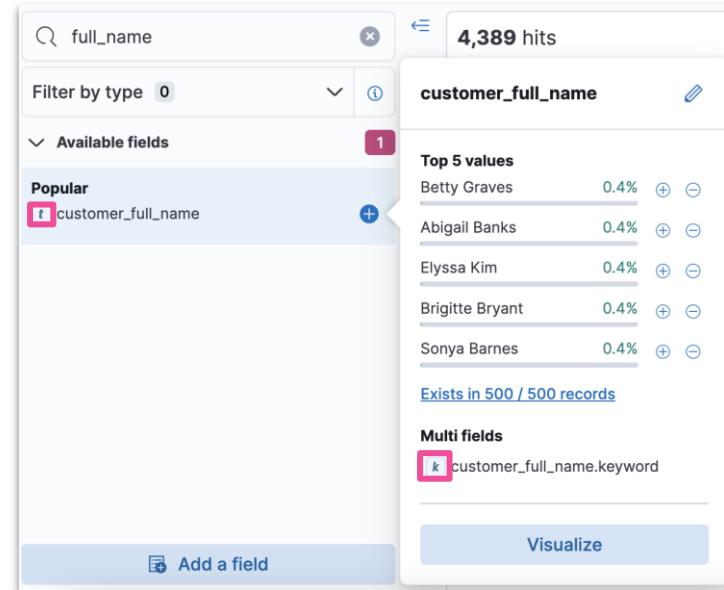


Fields (44)		Scripted fields (0)	Field filters (0)	Relationships (6)
<input type="text"/> Search				
Name ↑		Type		
hour_of_day ↴		long		
index		text		
index.keyword		keyword		
ip		ip		
ip_range		ip_range		
machine.os		text		
machine.os.keyword		keyword		
machine.ram		long		
memory		double		
message		text		

# Text vs. Keyword

- Strings can be indexed as both types
- Sometimes it is useful to have both types

TEXT	KEYWORD
Analyzed	Left as-is
Full text search	Filtering, Sorting, Grouping
email body, product description, etc.	IDs, email, hostnames, zip codes, tags, etc.



# Searchable vs Aggregatable

Kibana Sample Data eCommerce

Index pattern: kibana\_sample\_data\_ecommerce Time field: order\_date ★ Default

Fields (4 / 59) Scripted fields (0) Field filters (0) Relationships (6)

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
customer_first_name	text		<input checked="" type="checkbox"/>		<input type="checkbox"/>
customer_first_name.keyword	keyword		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
customer_full_name	text		<input type="checkbox"/>		<input type="checkbox"/>
customer_full_name.keyword	keyword		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Full text search

Exact term search

Aggregation

- Group
- Stats

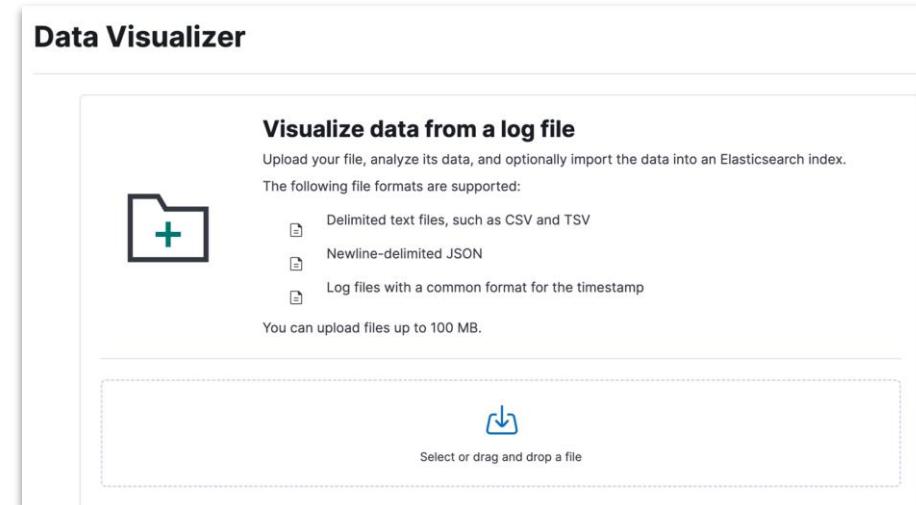
Sorting

Rows per page: 10 < 1 >

The screenshot shows the Kibana Fields table for the 'kibana\_sample\_data\_ecommerce' index pattern. It displays four fields: 'customer\_first\_name' (text), 'customer\_first\_name.keyword' (keyword), 'customer\_full\_name' (text), and 'customer\_full\_name.keyword' (keyword). The 'customer\_full\_name.keyword' field is highlighted with a pink box around its 'Type' column. The 'Searchable' and 'Aggregatable' columns for this field also have pink boxes around them, indicating they are both enabled. Other fields like 'customer\_first\_name' and 'customer\_full\_name' are shown with their respective types and status. A large pink arrow points from the 'customer\_full\_name.keyword' row towards the three pink boxes labeled 'Searchable', 'Aggregatable', and 'Excluded'. Another pink arrow points from the same row towards the three pink boxes labeled 'Full text search', 'Exact term search', and 'Aggregation'. A third pink arrow points from the 'customer\_full\_name.keyword' row towards the three pink boxes labeled 'Group', 'Stats', and 'Sorting'.

# Data Visualizer

- Understand your data
  - fields and associated data types
  - range
  - distribution
- Input
  - data view or saved search
  - file



# Data Visualizer

Query bar

Fields list

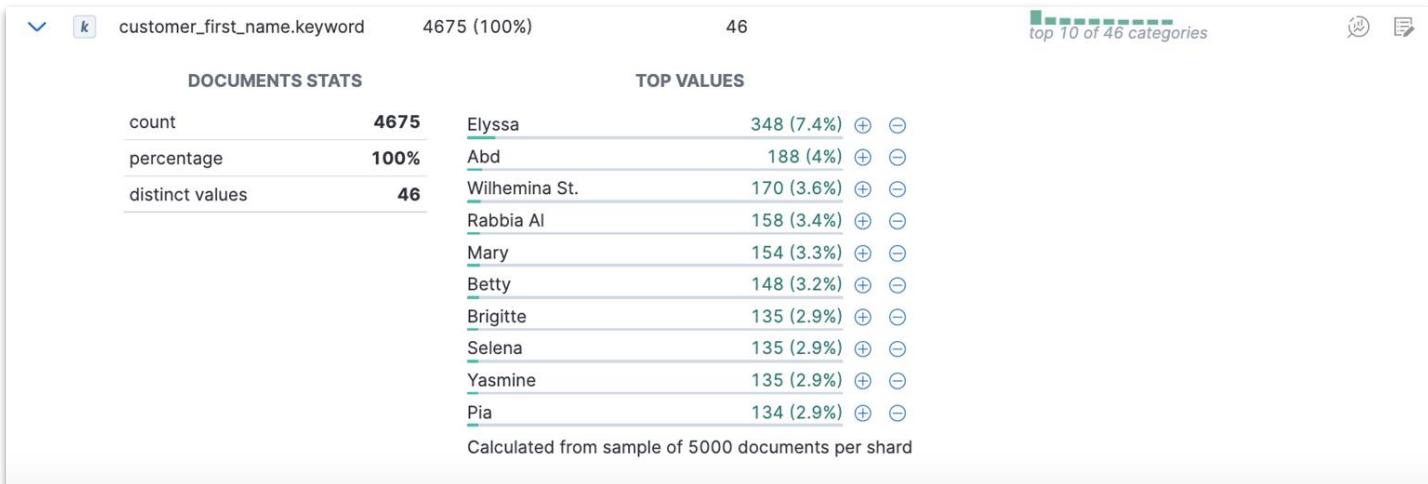
Time filter

The screenshot shows the Data Visualizer interface for the 'kibana\_sample\_data\_ecommerce' index. On the left, a sidebar menu includes 'Machine Learning', 'Overview', 'Anomaly Detection', 'Jobs', 'Anomaly Explorer', 'Single Metric Viewer', 'Settings', 'Data Frame Analytics', 'Jobs', 'Results Explorer', 'Analytics Map', 'Model Management', 'Trained Models', 'Nodes', 'Data Visualizer' (selected), 'File', and 'Data View'. The main area has three pink-highlighted sections: 'Query bar' pointing to the search bar at the bottom of the histogram; 'Fields list' pointing to the table below the histogram; and 'Time filter' pointing to the date range selector at the top right. The central part displays a histogram titled 'kibana\_sample\_data\_ecommerce' with the text 'Total documents: 4,675'. Below the histogram are search and sample size controls. The 'Fields list' table has columns for Type, Name, Documents (%), Distinct values, Distributions, and Actions. It lists fields like category, category.keyword, currency, customer\_first\_name, etc. A pink box labeled 'Histogram' covers the histogram area. To the right, there's an 'Explore your data' section with cards for 'Discover', 'Kibana sample data eCommerce', and 'Advanced anomaly detection'.

Type	Name	Documents (%)	Distinct values	Distributions	Actions
t	category	4675 (100%)	6	6 categories	
k	category.keyword	4675 (100%)	1	1 category	
t	currency	4675 (100%)	46	top 10 of 46 categories	
t	customer_first_name	4675 (100%)			
k	customer_first_name.keyword	4675 (100%)			
t	customer_full_name	4675 (100%)			

# Data Visualizer

- Filter for fields
  - by Name
  - by Type
- View Statistics
  - Document
  - Fields
  - Values Distribution



# Discover

- Explore and query data
  - search and filter the data
  - specify the time range
  - get information about the structure of the fields
- Create tables that summarize the contents of the data
- Customize and present your findings in a visualization on a dashboard
- Input
  - data view

The screenshot shows a modal window titled "Kibana Sample Data eCommerce" with a close button. Below the title are two buttons: "Add a field to this data view" and "Manage this data view". A section titled "Data views" contains a search bar labeled "Find a data view" and a "Create a data view" button. A list of data views is shown, with "Kibana Sample Data eCommerce" selected (indicated by a checkmark). Other listed data views include "Kibana Sample Data Flights" and "Kibana Sample Data Logs".

# Discover

The screenshot shows the Kibana Discover interface. At the top, there are three pink boxes with labels: "Fields list" pointing to the left sidebar, "Query bar" pointing to the search bar, and "Toolbar" pointing to the top right. The main area displays a histogram titled "4,373 hits" showing event counts over time from June 24th to July 23rd. Below the histogram, there are two tabs: "Documents" and "Field statistics". The "Documents" tab is selected, showing a table with one sorted document. The first document is from July 22, 2023, at 19:45:36.000. It contains detailed log data including fields like category, currency, customer\_id, and various timestamp and price details. The "Field statistics" tab is also visible. On the left sidebar, under "Popular fields", are products.manufacturer, products.price, products.product\_name, and total\_quantity. Under "Available fields", category is highlighted with a red arrow. Other available fields listed include currency, customer\_birth\_date, customer\_first\_name, customer\_full\_name, customer\_gender, customer\_id, customer\_last\_name, customer\_phone, day\_of\_week, #\_day\_of\_week\_i, email, and event.dataset. At the bottom of the sidebar is an "Add a field" button. The top right of the interface has a toolbar with Options, New, Open, Share, Alerts, Inspect, Save, Refresh, and a date range selector set to Jun 23, 2023 @ 20:39:02.912 → Jul 23, 2023 @ 14:58:21.796.

# Discover

Diagram illustrating the Kibana Discover interface with callouts pointing to key components:

- Data view**: Points to the left sidebar containing the "Popular fields" and "Available fields" sections.
- Query bar**: Points to the top search bar where you can filter data using KQL syntax.
- Time filter**: Points to the date range selector at the top right.
- Histogram**: Points to the histogram chart showing 4,373 hits over time.
- Doc table**: Points to the detailed document table view showing log entries.

The interface includes a header with "Discover" and various navigation buttons (Options, New, Open, Share, Alerts, Inspect, Save, Refresh), a search bar, and a histogram showing 4,373 hits from June 24th to July 23rd. The document table displays log entries for two specific dates: Jul 22, 2023 @ 19:45:36.000 and Jul 22, 2023 @ 19:31:12.000, with rows per page set to 100.

4,373 hits

Jun 23, 2023 @ 20:39:02.912 → Jul 23, 2023 @ 14:58:21.796 (interval: Auto ~ 12 hours)

Documents Field statistics

1 field sorted

order\_date

Jul 22, 2023 @ 19:45:36.000

Jul 22, 2023 @ 19:31:12.000

Add a field

Rows per page: 100 < 1 2 3 4 5 >

# Context: time and data view

- No results ?
- Always check the **time filter** and the **data view**
  - The combination of these is your **context**

**No results match your search criteria**

Here are some things to try:

- Expand the time range
- Remove or [disable filters](#)

[View all matches](#)



# Working with fields

- Filter for field
  - by **name**
  - by **type**
- View **top values**
- Field areas
  - **Selected fields:** fields added to document table
  - **Popular fields:** commonly used fields
  - **Available fields:** all fields
  - **Empty fields:** fields that have no data in the selected time range
  - **Meta fields:** fields that contain metadata

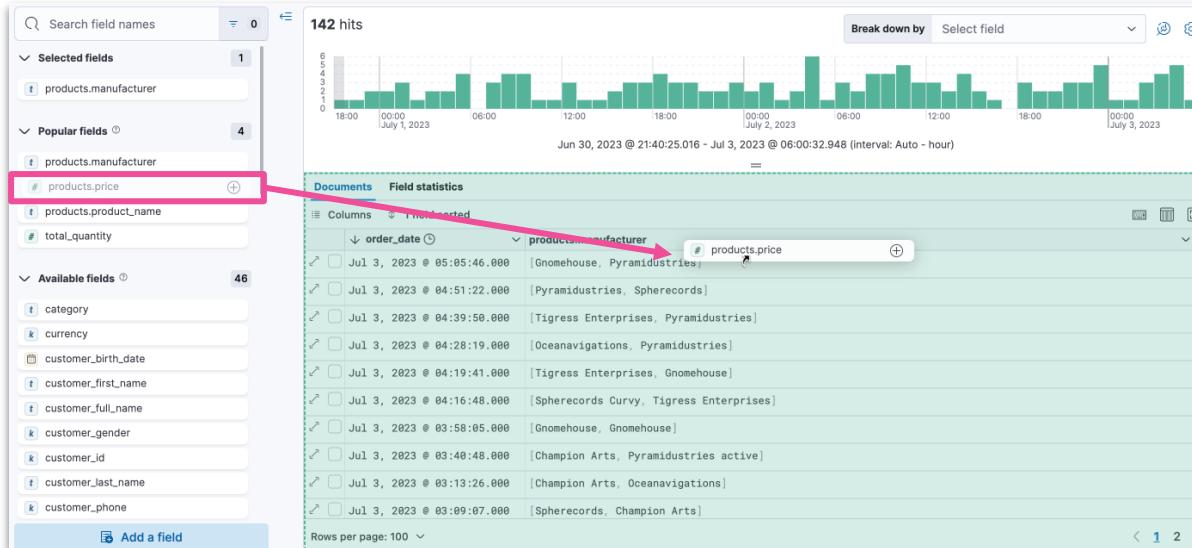
The screenshot shows the Elasticsearch Settings interface with the following sections and their contents:

- Selected fields:** Contains fields: category (text), products.price (number), products.product\_name (text).
- Popular fields:** Contains fields: products.manufacturer (text), products.price (number), products.product\_name (text), total\_quantity (number).
- Available fields:** Contains fields: category (text), currency (keyword).
- Empty fields:** Message: "There are no empty fields."
- Meta fields:** Contains fields: \_id (keyword), \_index (keyword), score (number).

A pink callout box labeled "Data type" has arrows pointing to the category field in each of the three main sections (Selected fields, Popular fields, and Available fields).

# Document table

- To create columns in the document table
  - drag and drop fields from the fields list
  - Click the + next to the field



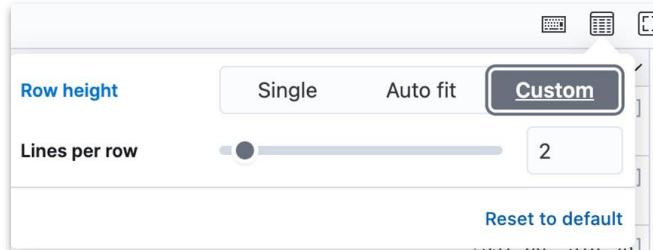
# Organize the table

- Organize table columns
  - move
  - resize
  - copy
  - sort
  - edit
- Set display settings

Documents Field statistics

Columns 1 field sorted

	↓ order_date ⓘ	products.manufacturer	
↗	Jul 3, 2023 @ 05:56:10.000	[Microlutions, Micro...]	<input type="button" value="Remove column"/>
↗	Jul 3, 2023 @ 05:27:22.000	[Low Tide Media, Elit...]	<input type="button" value="Sort A-Z"/>
↗	Jul 3, 2023 @ 05:05:46.000	[Gnomehouse, Pyramid...]	<input type="button" value="Sort Z-A"/>
↗	Jul 3, 2023 @ 04:51:22.000	[Pyramidustries, Sph...]	<input type="button" value="Move left"/>
↗	Jul 3, 2023 @ 04:39:50.000	[Tigress Enterprises]	<input type="button" value="Move right"/>
↗	Jul 3, 2023 @ 04:32:38.000	[Elitelligence, Elite...]	<input type="button" value="Copy name"/>
↗	Jul 3, 2023 @ 04:28:19.000	[Oceanavigations, Pyramidustries]	<input type="button" value="Copy column"/>



# Document table

- Expand for details
- View as
  - Table
  - JSON
- Single document
- Surrounding documents

Expanded document

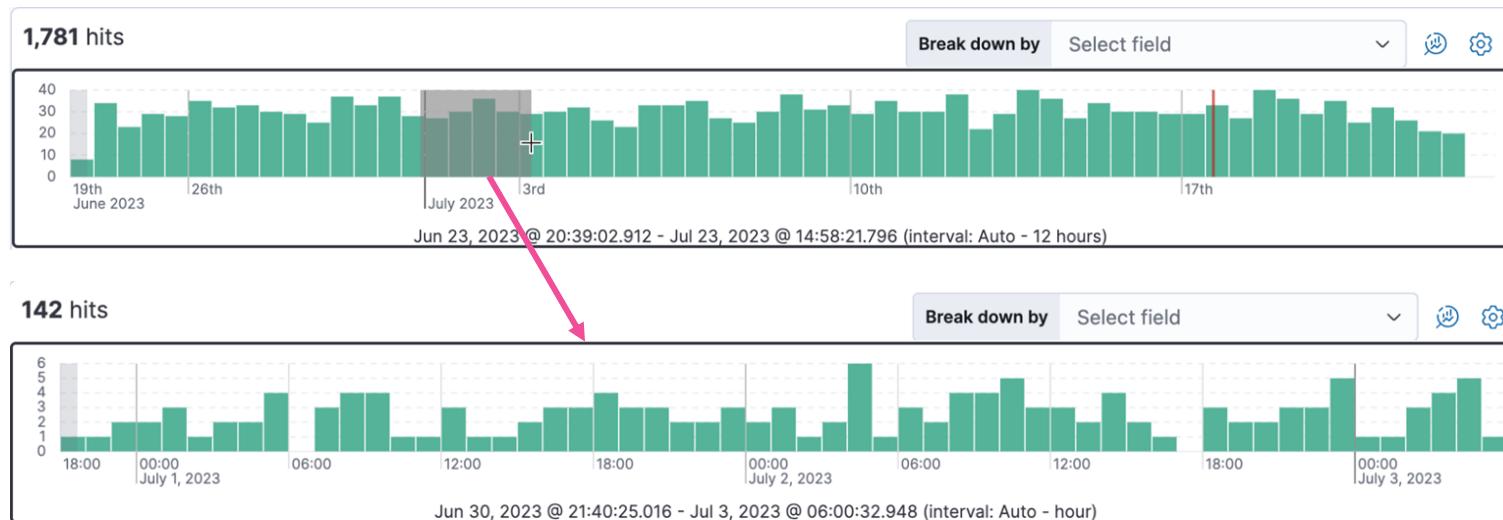
View: [Single document](#) [Surrounding documents](#) [?](#)

1 of 27

Actions	Field	Value
	<code>k _id</code>	pBVqLlKBF3Qm8ujF8zhA
	<code>k _index</code>	kibana_sample_data_ecommerce
	<code># _score</code>	-
	<code>t category</code>	[Women's Accessories, Women's Shoes]
	<code>k currency</code>	EUR
	<code>t customer_first_name</code>	rania
	<code>t customer_full_name</code>	rania Nash
	<code>k customer_gender</code>	FEMALE
	<code>k customer_id</code>	24
	<code>t customer_last_name</code>	Nash
	<code>k customer_phone</code>	(empty)
	<code>k day_of_week</code>	Monday

# Interactive histogram

- The time filter can be visually changed by:
  - **click and dragging** across the histogram
  - **clicking** on a single bar



# Summary: Discover and Data Visualizer

Module 2 Lesson 1

# Summary

- Data **types** influence how fields may be used in Kibana
- The **Data Visualizer** can be used to view your data as a whole
- **Discover** can be used to drill down into specific documents
- The **time filter** and **data view** in Discover form the context of the view
  - If no data is visible, check the time and pattern
- The document table can be customized to show selected fields

# Quiz

1. In Discover, which two settings determine the scope or context?
2. **True or False:** The Data Visualizer tool can be used to examine specific documents.
3. What data type is represented by this icon: 

# Discover and Data Visualizer

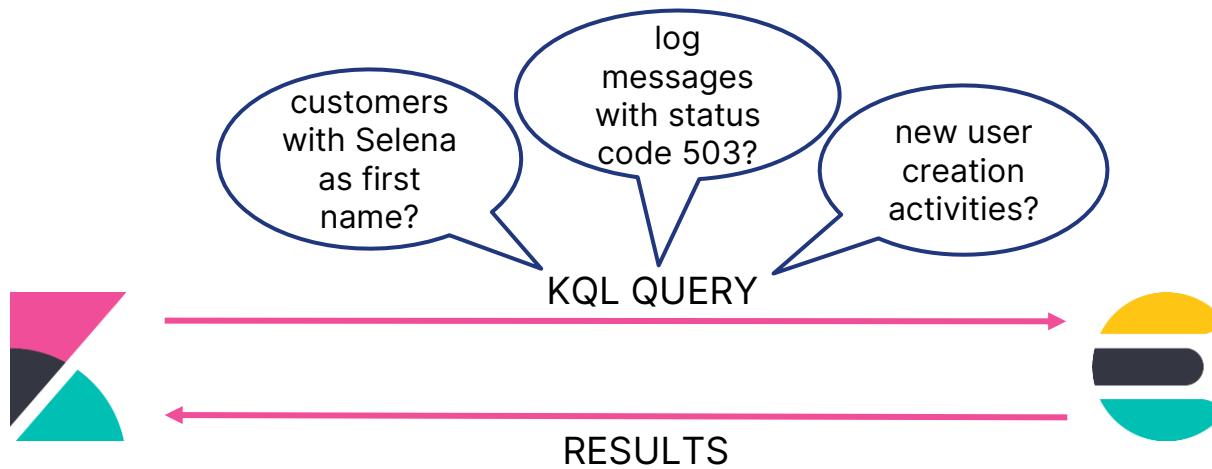
Lab 2.1 - Explore logs data with Discover and Data Visualizer

# KQL and filters

Module 2 Lesson 2

# Search recap

- A search is executed by sending a **query** to Elasticsearch
  - a query can answer many different types of **questions**
- In Kibana, a search can be executed using **KQL**, the Kibana Query Language

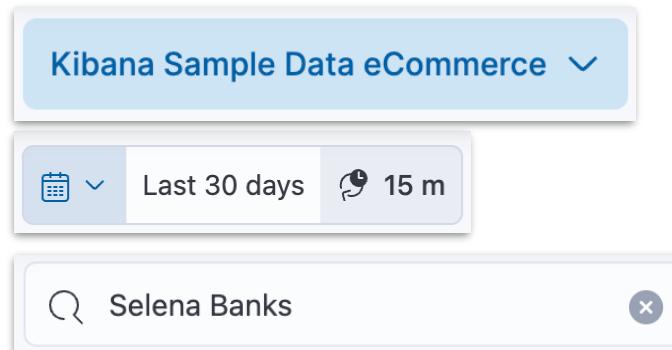


# Query context

- Search result quality depends on the quality of query
  - crafting a good question gets good results

Find all the orders for last month from customer “Selena Banks”

- Establish context
  - Data view
  - Time range



- Define Query

# Better queries, better results

- Our search returns a lot of results
  - But not the exact results
- By default, the query logic is going to look in all fields, and for any values, leading to results like...

	↓ order_date ⓘ	customer_first_name	customer_full_name	customer_last_name
↗	Jul 21, 2023 @ 23:28:48.000	Robert	Robert Banks	Banks
↗	Jul 21, 2023 @ 16:36:58.000	Selena	Selena Rose	Rose
↗	Jul 21, 2023 @ 10:52:48.000	Muniz	Muniz Banks	Banks
↗	Jul 21, 2023 @ 02:12:58.000	Selena	Selena Boone	Boone
↗	Jul 20, 2023 @ 17:04:19.000	Selena	Selena Banks	Banks
↗	Jul 20, 2023 @ 13:47:02.000	Selena	Selena Mcdonald	Mcdonald
↗	Jul 20, 2023 @ 09:58:05.000	Selena	Selena McCarthy	McCarthy
↗	Jul 20, 2023 @ 08:04:19.000	Selena	Selena Roberson	Roberson
↗	Jul 20, 2023 @ 07:00:58.000	Abigail	Abigail Banks	Banks

# Queries precision

## FREE TEXT SEARCH

- Matched by all fields by default
- Inefficient
- Imprecise results

A screenshot of a search interface. The search bar contains the query "Selena Banks". Below the search bar, the text "151 hits" is displayed.

vs

## FIELD SPECIFIC SEARCH

- Only fields specified will be matched
- More efficient
- Will yield precise results
- Can take advantage of **KQL suggestions**

A screenshot of a search interface. The search bar contains the query "customer\_full\_name: \"Selena Banks\"". A pink callout box with the text "In quotes" has an arrow pointing to the quote marks in the search bar. Below the search bar, the text "2 hits" is displayed.

# Boolean operators

- **and, or, not**
- **and** takes precedence over **or**
- Group operators and terms using parentheses

full name  
contains Selena  
**or** Banks

quotes  
omitted

customer\_full\_name: Selena Banks

full name  
contains Selena  
**and** Banks **in**  
**that order**

In quotes

customer\_full\_name: "Selena Banks"

full name  
contains Selena  
**and** Banks **not**  
**necessarily in**  
**that order**

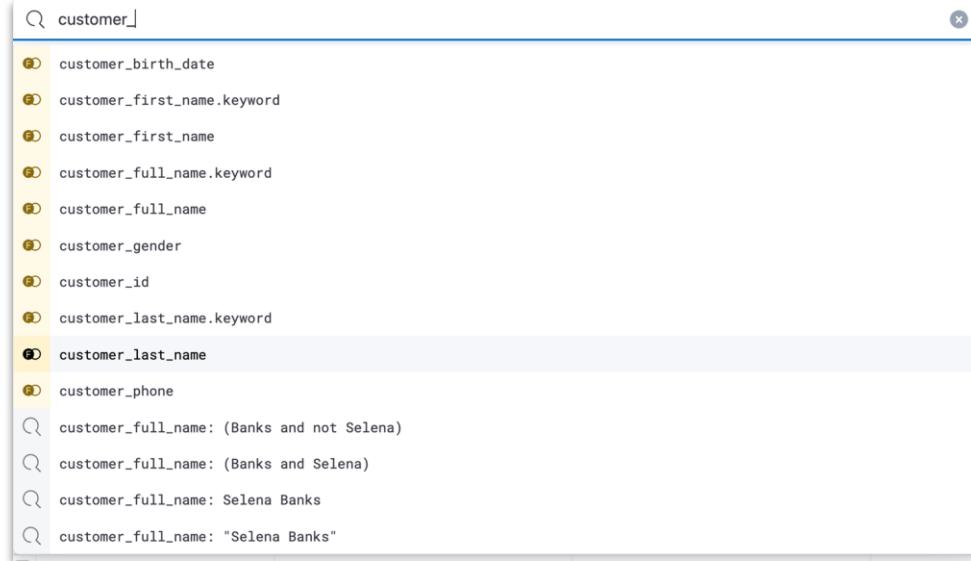
customer\_full\_name: (Banks and Selena)

full name  
contains Banks  
**and does not**  
contain Selena

customer\_full\_name: (Banks and not Selena)

# KQL suggestions

- KQL auto-suggests
  - field names
  - values
  - operators
  - previously used queries



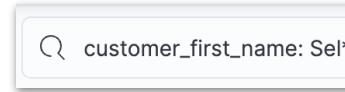
The screenshot shows the KQL editor interface. On the left, a dropdown menu lists suggestions for 'category.keyword': category.keyword, products.category.keyword, :, : \*, and, or. Below the suggestions, there are descriptions for each operator: '=' means 'equals some value', ': \*' means 'exists in any form', 'and' means 'Requires both arguments to be true', and 'or' means 'Requires one or more arguments to be true'. An arrow points from this editor to a separate search interface on the right.

The right side shows a search bar with the query 'category.keyword: M'. Below the search bar is a list of results: "Men's Accessories", "Men's Clothing", and "Men's Shoes".

# Wildcard query

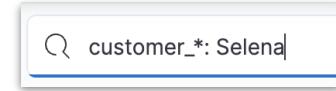
- Wildcard \* used to

- search by a term prefix



customers  
with first  
name starting  
with **sel**

- search multiple fields



any of the fields  
that start with  
**customer\_**  
contains **Selena**

# Range query

- For numeric and date types
  - `>`, `>=`, `<` and `<=` are supported
  - date math expressions are supported

orders executed **on or before 21 June 2023**  
where price is less than or equal to **\$50** and **more than 3 unique products** were purchased

🔍 `products.taxful_price <= 50 and total_unique_products > 3 and order_date <= "2023-06-21"`

orders executed  
**in the last 4 days**

🔍 `order_date > now-4d`

orders that contained  
products created **during the month starting 14 November 2016**

🔍 `products.created_on > 2016-11-14 and products.created_on < 2016-11-14||+1M/d`

# Query bar limitations

- Let's take our query example and expand it
  - **customer\_full\_name:"Selena Banks"**
  - **taxful\_total\_price>=50**
  - **geoip.city\_name: Los Angeles**
  - **category:Women's Shoes**
- You may want to use different combinations of these clauses
- With the query bar, you will have to do a lot of typing and deleting
- Filters are **sticky** queries
  - individual query clauses that can be turned on and off

# Define a filter

- There are two ways to define a filter from Discover
  - **Add filter (+)** link will open a dialog
  - + or - symbol on any list creates a filter for that value

The screenshot illustrates two methods for defining filters in the Elasticsearch Discover interface:

- Method 1 (Left): Using the 'Add filter' dialog.**
  - A modal window titled "Add filter" is open. The "Field" dropdown is set to "Select a field first". The "Operator" dropdown is set to "Waiting". A pink box highlights the blue "+ Add filter" button in the top-left corner of the modal.
  - Below the modal, the main Discover interface shows a search bar with "Filter your data using KQL syntax" and a time range of "Last 30 days".
  - At the bottom of the interface, there is a row of filters: "Jul 20, 2023 @ 17:04:19.000", "Selena", and "Banks". The "Selena" filter has a pink box around it, and the "Banks" filter has a pink box around it. A cursor is hovering over the "Selena" filter.
- Method 2 (Right): Using the "Top values" chart.**
  - A chart titled "customer\_first\_name" shows the distribution of first names. The y-axis is labeled "Top values". The data is:

customer_first_name	Percentage
Selena	85.4%
Abigail	2.0%
Muniz	2.0%
Betty	1.3%
  - A pink arrow points from the "Selena" entry in the chart to the blue "+" button next to it, indicating that clicking this button adds the filter "customer\_first\_name: Selena" to the current query.

# Defining complex filters

- Create and apply multiple filters simultaneously
  - use for nested queries
  - select logical OR and AND operators

The screenshot shows the 'Add filter' dialog in 'Technical preview' mode. A pink arrow points to the first 'AND' operator between the 'category.keyword' and 'taxful\_total\_price' filters. Below the filters, a 'Preview' section displays the resulting query: 'category.keyword: Women's Shoes AND taxful\_total\_price: \$50 to +∞'. The 'Custom label (optional)' field contains 'Complex filter'. At the bottom right are 'Cancel' and 'Add filter' buttons.

Add filter Technical preview Edit as Query DSL

= category.keyword is Women's Shoes AND  
= taxful\_total\_price is between 50 → End

**Preview**  
category.keyword: Women's Shoes AND taxful\_total\_price: \$50 to +∞

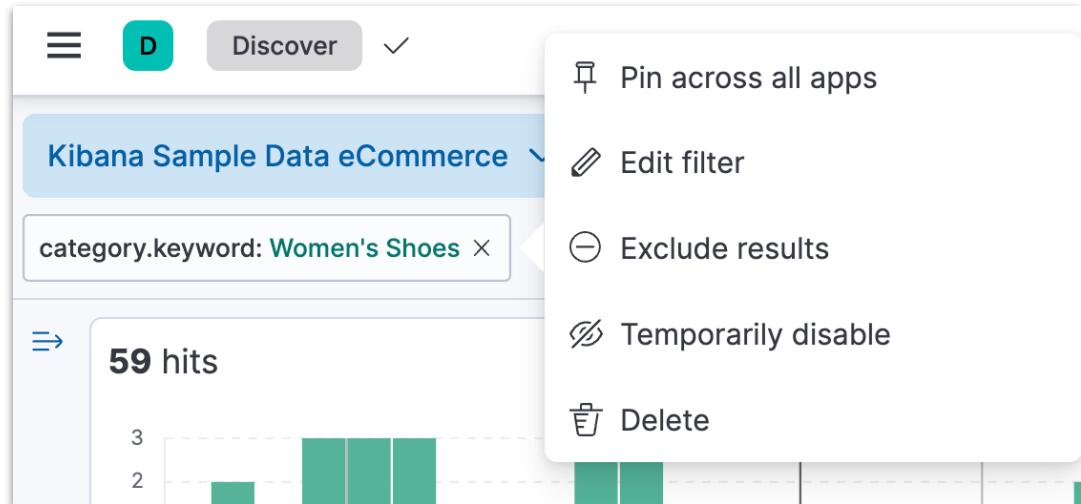
Custom label (optional)  
Complex filter

Cancel Add filter

# Filter operations

- Once defined, a filter can be:

- pinned
- edited
- negated
- disabled
- deleted



- Filters can be collectively managed via the  icon

# Editing filters

- Internally filters are transformed into a query
- You can change the filter by editing the query
- You can add a custom a label to the filter to quickly identify it

The screenshot shows the Kibana Discover interface. On the left, there's a sidebar with a 'Popular fields' section containing 'products.manufacturer', 'products.price', 'products.product\_name', and 'total\_quantity'. The main area shows a search bar with 'category.keyword: Women's Shoes AND taxful\_total\_price: \$50 to +∞'. Below it, a histogram shows '24 hits' for the date 'April 30, 2024' with bins at 13:00 and 14:00. A modal window titled 'Edit filter' is open, showing the query language: 'category.keyword is Women's Shoes' AND 'taxful\_total\_price is between 50 End'. A 'Custom label (optional)' field contains 'Women's shoes >= \$50', which is highlighted with a pink rectangle. The modal has 'Cancel' and 'Update filter' buttons.

# Filters and query bar

- You can use filters and KQL together
  - use KQL for broad search
  - use filters to zero in on subset
    - enable, include, exclude as needed

The screenshot shows the Kibana interface for the Sample Data eCommerce dataset. At the top, there is a search bar containing the query "customer\_full\_name: 'Selena Banks'". Below the search bar are four filter cards: "category.keyword: Women's Shoes", "taxful\_total\_price: \$50 to +∞", "NOT geoip.city\_name: Los Angeles", and "manufacturer: Tigress Enterprises".

	↓ order_date (🕒)	customer_f...	customer_f...	customer_l...	category	taxful_total...	geoip.city_...
↗	Jul 20, 2023 @ 17:04:19.000	Selena	Selena Banks	Banks	[Women's Shoes, Women's Accessories]	\$53.97	Marrakesh

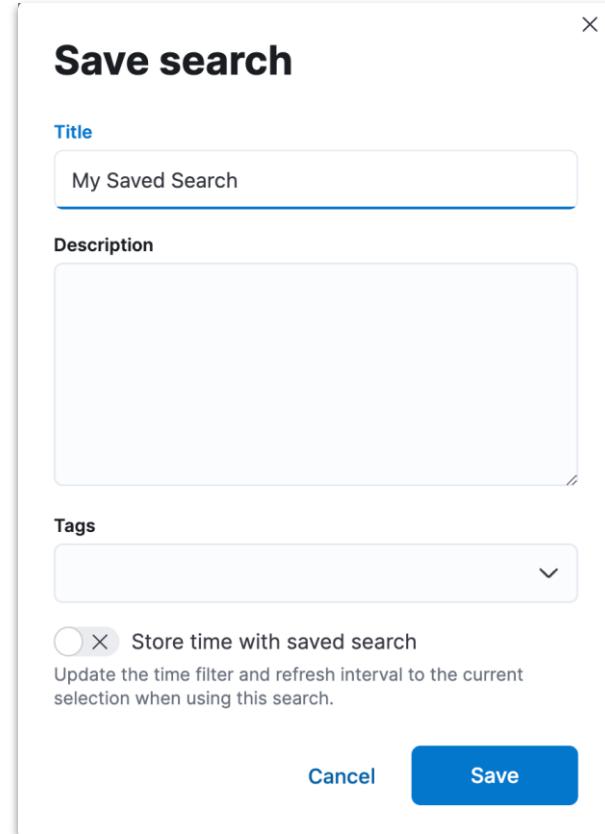
# Break down histogram by value

- Break down fields by value
- Creates a filter in the filter list
- Click on a bar section to select filters



# Saved searches

- Reuse of search in Discover
- Add search results to dashboard
- Use as source for visualization
- Stores
  - query text
  - filter
  - time
  - Discover view
    - data view
    - columns selected
    - sort order



# Saved queries

- Reuse queries anywhere a query bar is present
- Saves
  - query text
  - filters (optional)
  - time range (optional)

< **Save as new**

**Name**

My Saved Query

Name cannot contain a leading or trailing whitespace and must be unique.

Include filters

Include time filter

**Save query**

# Saved query vs. saved search

SAVED SEARCH	SAVED QUERY
<p>Includes Discover view</p> <ul style="list-style-type: none"><li>● columns in document table</li><li>● sort order</li><li>● data view</li></ul>	Discover view is not included
Can be added as a panel to a dashboard	Can be loaded where a query bar is present including dashboard
Can store KQL queries, filters, time filter, and refresh interval	Can store KQL queries, filters and time filter
Can be shared (copied) between spaces	Can be shared (copied) between spaces

# Summary: KQL and filters

Module 2 Lesson 2

# Summary

- Kibana filters and the query bar are complementary
- Kibana filters provide an easy way to explore data by
  - enabling and disabling them
  - pinning and having them follow to different parts of Kibana
- The query bar can be used to search all the data inside Elasticsearch
- The KQL language supports **and**, **or** and **not** boolean operators
- KQL provides auto-completion for writing queries
- Queries and searches can be **saved** for later reuse

# Quiz

1. **True or False:** You can only use a single filter at a time in Kibana.
2. Name three actions that you can perform on a filter?
3. What are three different boolean operators you can use in a KQL query.

# KQL and filters

Lab 2.2 - Query and filter the logs data with KQL

# Field focus

Module 2 Lesson 3

# Visualization basics

- Visualize straight from fields list

- Lens

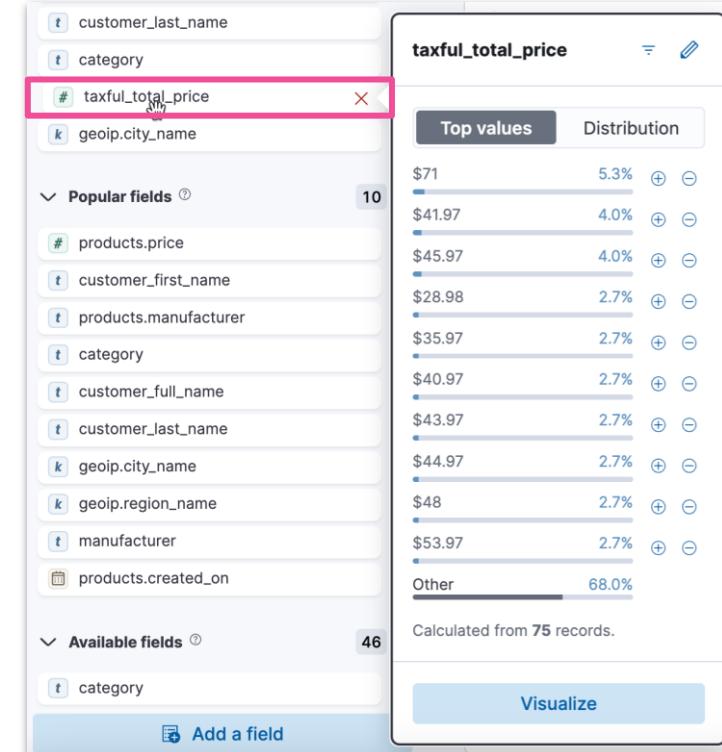
- explore suggestions
    - change visualization type
    - change layer settings (e.g., # of top values)
    - And more...

- maps for Geo data

- Save to panels on the dashboard
- Use filters in the dashboard
- Change time filter interactively

# The shortest path to visualization

- Visualizations can be created directly from Discover or Data Visualizer
- Select a field, and click **Visualize** [Discover] or icon [Data Visualizer]
  - geo point fields will open in **Maps**
  - all other field types will open in **Lens**



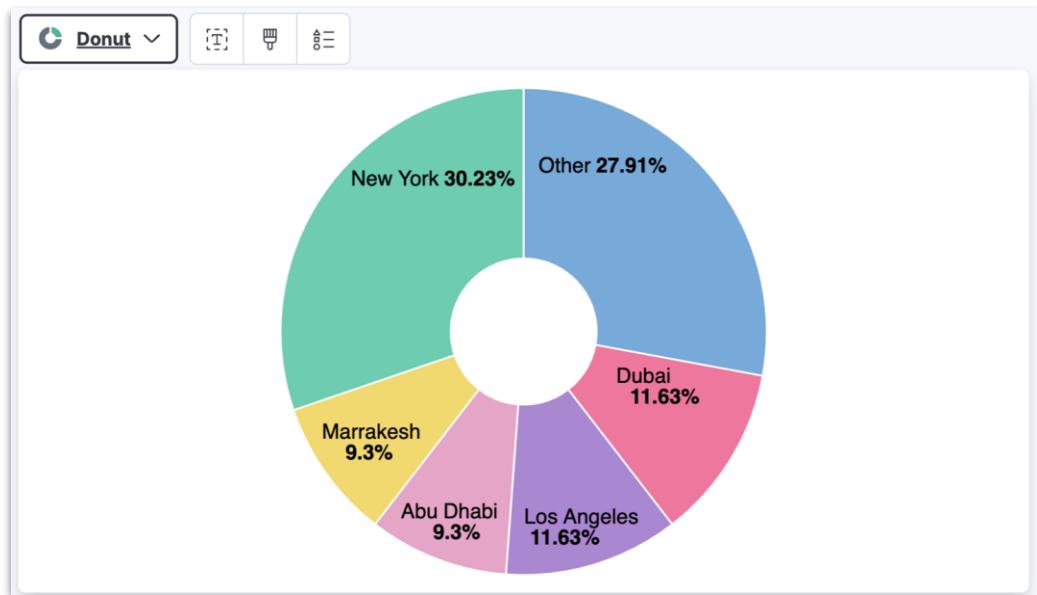
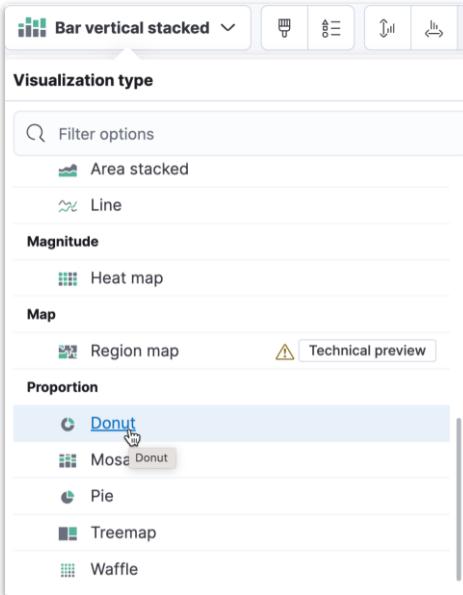
# Focus with Lens

- We will use Lens to focus on a single field: **geoip.city\_name**
- If we **Visualize** this field, we are presented with this view...
- Vertical bar chart
- Simple count of records
- Split by city name
- Sorted descending
- Top 5 shown
- With an “Other”



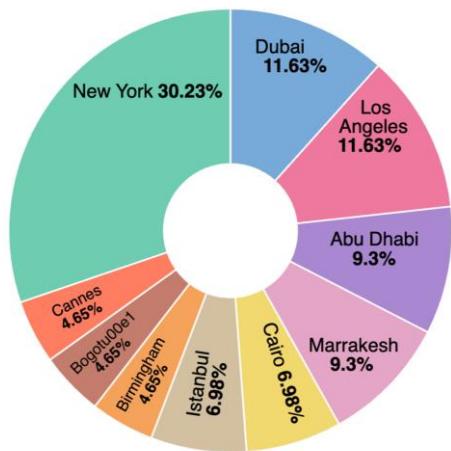
# Change the visual

- Bar charts are nice, but sometimes it helps to see a proportion
- Change the view to a **Donut**



# Change the values

- Maybe we don't want Other, or want more than 5 cities
- In the **layer pane**, click **Slice by** to adjust the slices



Donut

Kibana Sample Data eCommerce

Slice by

Optional

Top 5 values of geoip.city\_name

+ Add or dr

Metric

Count of records

Slice

Data

Functions

Date histogram

Intervals

Filters

Top values

Fields

= geoip.city\_name

+ Add field

Number of values

10

Rank by

Count of records

Rank direction

Ascending

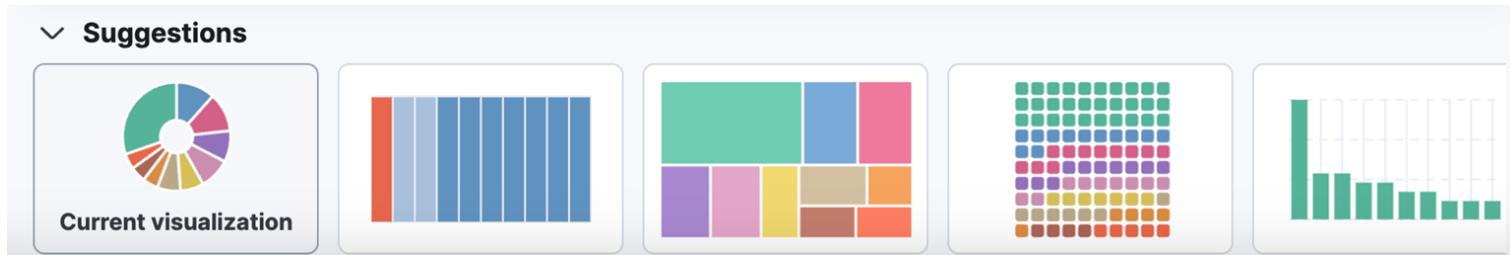
Descending

Collapse by

X Close

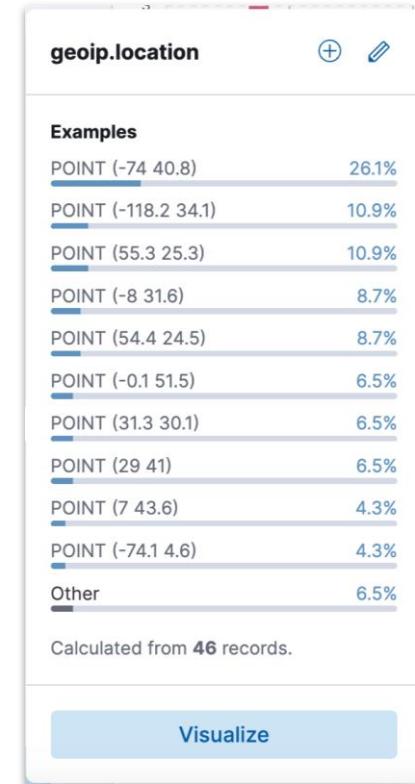
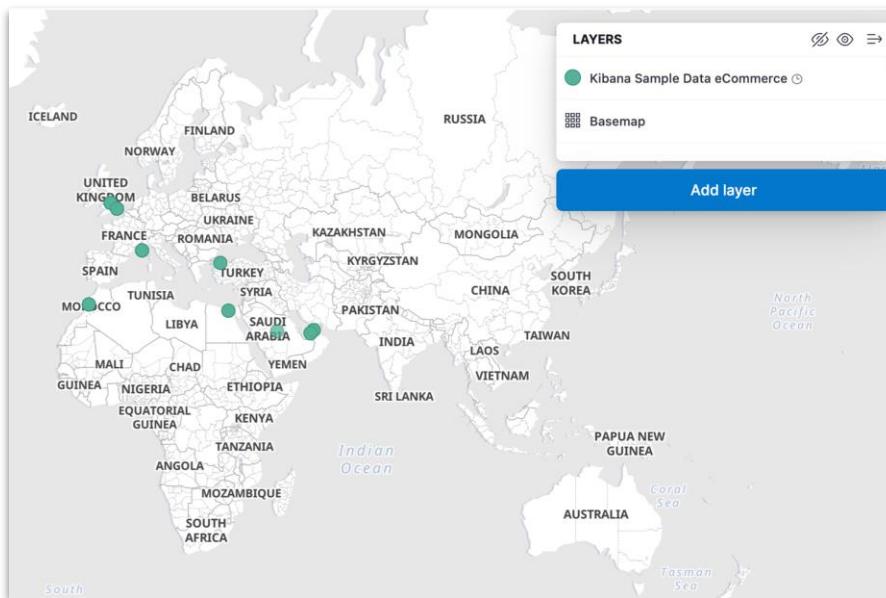
# Get suggestions

- Everyone loves donuts, but maybe a tree map looks better
- See a preview in the **Suggestions** panel
- Select the view that works best for you



# Map your data

- **Visualize** a geo point field to open the **Map editor**
- We will spend more time with Maps in later lessons



# Using visualizations

- Visualizations can be saved
  - and automatically added to a **dashboard**
- Lens and Maps visualizations can create **filters**
  - filters can be pinned and used in **Discover**
- Click and drag in time based visualizations to change the **time filter**
  - just like the **Discover** histogram

# Summary: Field focus

Module 2 Lesson 3

# Summary

- The **Visualize** link in Discover creates **Lens** or **Maps** visualizations
- **Lens** enables you to visualize a field
- **Maps** visualizations link documents to points on a map
- Visualizations can be used to create **filters** and change the **time filter**
- Visualizations can be saved to **dashboards**

# Quiz

- 1. True or False:** Visualizing geo point data opens the Lens editor by default.
2. What part of Lens would you use to change the number of displayed values.
- 3. True or False:** It is difficult to change visualization styles in Lens.

# Field focus

Lab 2.3 - Create visualizations from Discover

# Data Analysis with Kibana: Agenda

- Getting Started
- Search your Data
- **Visualize your Data**
- Additional Visualizations
- Present your Data
- Analyze your Data with Machine Learning
- Advanced Kibana
- Alerting

# Visualize your Data

Module 3

# Topics

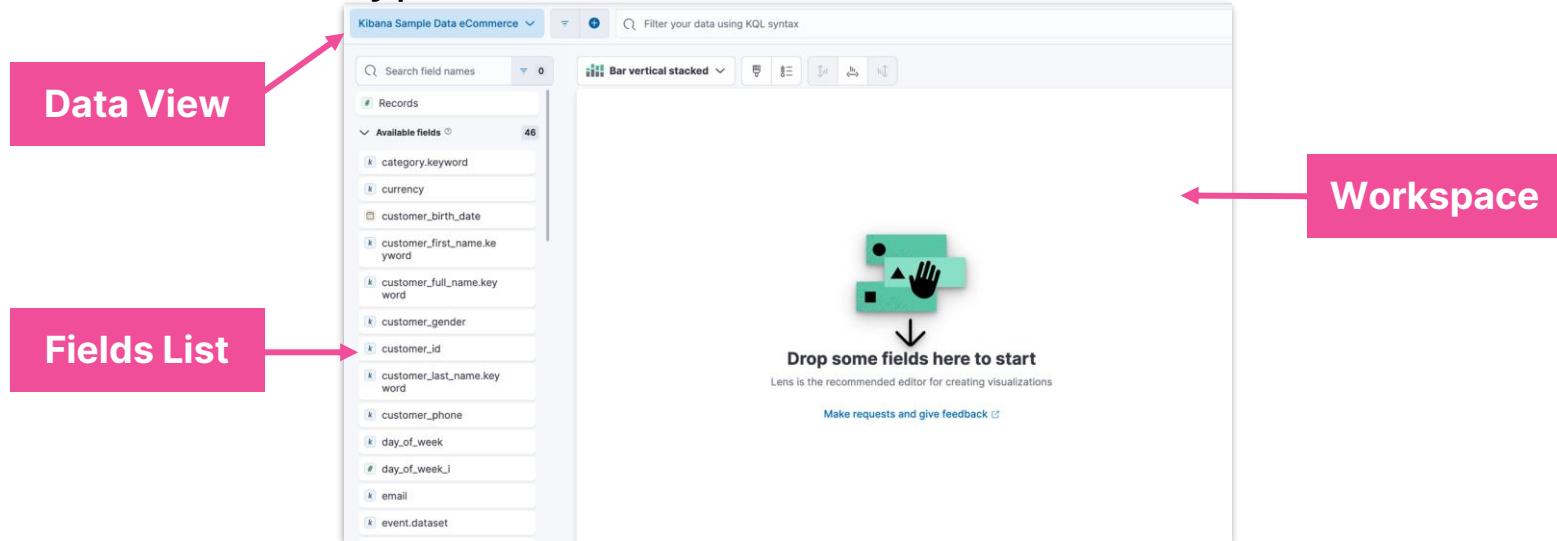
- Create visualizations
- Adjust visualizations
- Create maps

# Create visualizations

Module 3 Lesson 1

# Lens Review

- Lens is the default editor for creating new visualizations
  - direct access from dashboards
  - most data types from Discover



# Lens advantages

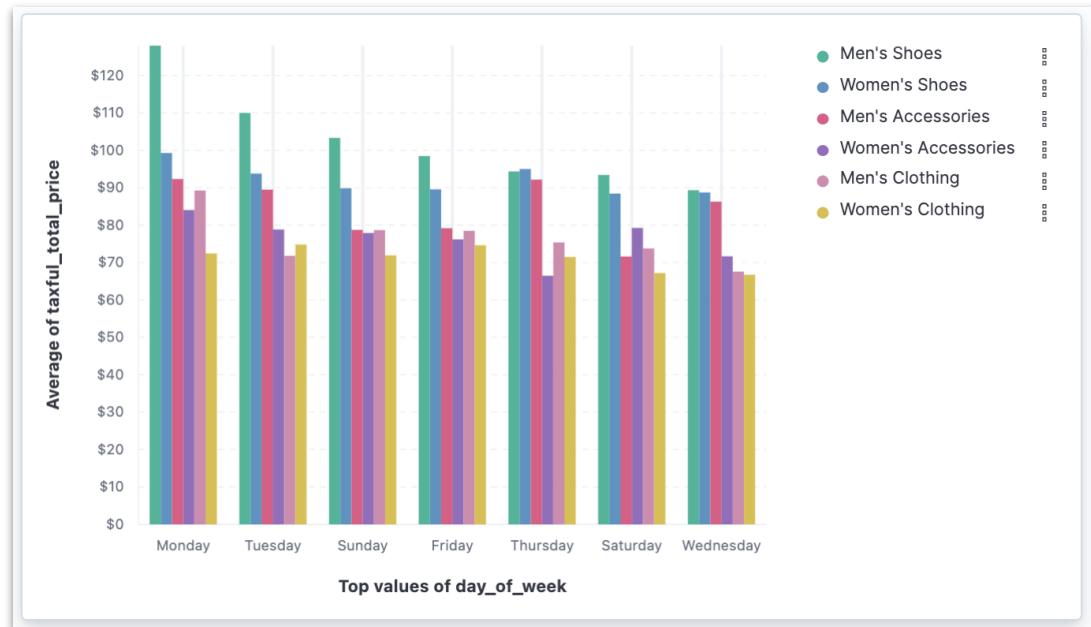
- Switch anytime
  - visualization type
  - data view
- Suggestions based on data type
- Compare different data sources
- Combine multiple fields

The screenshot shows the Kibana Lens configuration interface. A pink callout box labeled "Data view" points to the top section where "Bar vertical stacked" is selected from a dropdown menu. Another pink callout box labeled "Layer pane" points to the bottom right corner where a blue button labeled "Add layer" is located. A third pink callout box labeled "Visualization type" points to the top right corner where "Kibana Sample Data eCommerce" is selected from another dropdown menu. The interface includes sections for "Horizontal axis" (Optional), "Vertical axis", and "Breakdown" (Optional), each with a "Add or drag-and-drop a field" button.

# An example

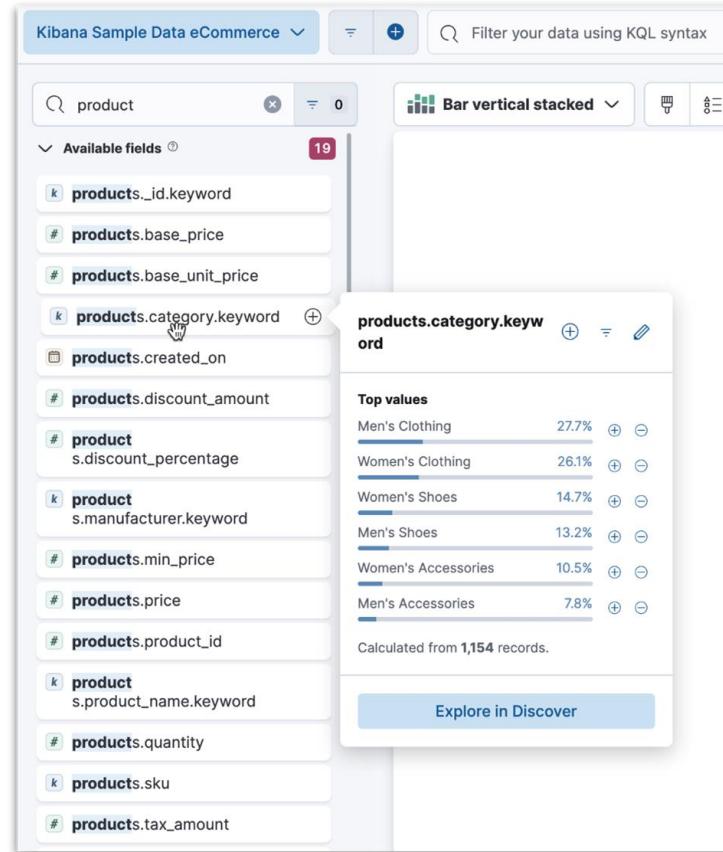
- Explore fields list
- Drag and drop fields
  - workspace
  - axes
- Adjust
  - # of top values
  - functions
  - advanced

Average total price broken down by day and category



# Fields List

- Fields list
  - similar to Discover
  - search field names
  - filter by type
  - click to view top values
- To add to Workspace
  - drag and drop field
  - click +



# Visualization type and options

## 1. Visualization Type

- Tabular
- Bar
- Goal and single value
- Line and Area
- Magnitude
- Map
- Proportion

## 2. Visual options and legend

## 3. Axis settings

The screenshot shows the 'Visualization type' section of the Elasticsearch visualization configuration. At the top, there is a dropdown menu labeled 'Bar vertical' with a downward arrow. To the right of the dropdown are three small icons: a bar chart icon (circled in pink), a grid icon, and a double-headed arrow icon. Below the dropdown is a search bar with the placeholder 'Filter options'. The main area is divided into sections: 'Tabular' (containing 'Table'), 'Bar' (containing 'Bar horizontal', 'Bar horizontal percentage', 'Bar horizontal stacked', 'Bar vertical' - which is highlighted with a blue selection bar and has a checkmark icon to its left, and 'Bar vertical percentage', 'Bar vertical stacked'), and 'Goal and single value' (containing 'Gauge horizontal' and 'Gauge vertical', each with a yellow warning icon and the text 'Technical preview' next to it). A vertical scrollbar is visible on the right side of the main content area.

# Layer pane

- The layer pane lets you customize the **data**
  - generally defaults to a **count** based on **date** or **top values**
  - limited switching of the visualization can be done as well
- Various visualization types have different **field groups**

The screenshot shows the Kibana Layer pane with the following configuration:

- Visualization Type:** Bar vertical stacked
- Data Source:** Kibana Sample Data eCommerce
- Horizontal axis:** Top 5 values of products.category.keyword
- Vertical axis:**
  - Count of records
  - Median of taxful\_total\_price
- Add or drag-and-drop a field:** + Add layer
- Breakdown:** Top 3 values of day\_of\_week
- Add layer:** Add layer

Annotations on the right side explain the options:

- Bar, line, area, and heatmap** have horizontal axis, vertical axis and breakdown
- Metrics** have a single and multiple metric
- Proportions** have grouping and sizing
- Tables** have rows, columns and metrics
- Options differ based on visualization type

# Add multiple layers

- Add layers with **same** or **different** Data views
- Change visualization
  - options change based on type
- Can also clone layers

**Pie**

Kibana Sample Data eCommerce

Slice by

- Top 5 values of products.category.keyword
- Top 7 values of day\_of\_week
- + Add or drag-and-drop a field

Metric

Count of records

Bar vertical stacked

Kibana Sample Data eCommerce

Horizontal axis

Optional  
Top 5 values of products.category.keyword

Vertical axis

Count of records

+ Add or drag-and-drop a field

Breakdown

Optional  
Top 7 values of day\_of\_week

+ Add layer

Table

Kibana Sample Data eCommerce

Rows

Optional  
Top 5 values of products.category.keyword  
Top 7 values of day\_of\_week  
+ Add or drag-and-drop a field

Split metrics by

Optional  
Top 3 values of geoip.continent\_name  
+ Add or drag-and-drop a field

Metrics

Count of records  
Median of taxful\_total\_price  
+ Add or drag-and-drop a field

# Axis settings

- For Bar, Line and Area charts
- Functions / Formula
  - Aggregation / Grouping
  - Math on Aggregated data
- Display Settings
  - Name (Label)
  - Value format
  - Series color
  - Axis side

Appearance

Name	Median of taxful_total_price
Value format	Default
Series color	<input type="checkbox"/> Auto
Axis side	Left      Auto      Right

Horizontal axis

Data

Functions 1

Date histogram • Intervals • Top values

Filters

Vertical axis

Data

Method

Quick function      Formula

Functions 1

Average	Minimum
Count	Moving average
Counter rate	Percentile
Cumulative sum	Percentile rank
Differences	Standard deviation
Last value	Sum
Maximum	Unique count
Median	

# Quick functions

- Use quick functions to apply aggregations to data
  - summarize your data as metrics, statistics, or other analytics
  - available functions depend on the selected field

Quick function      Formula

Functions 

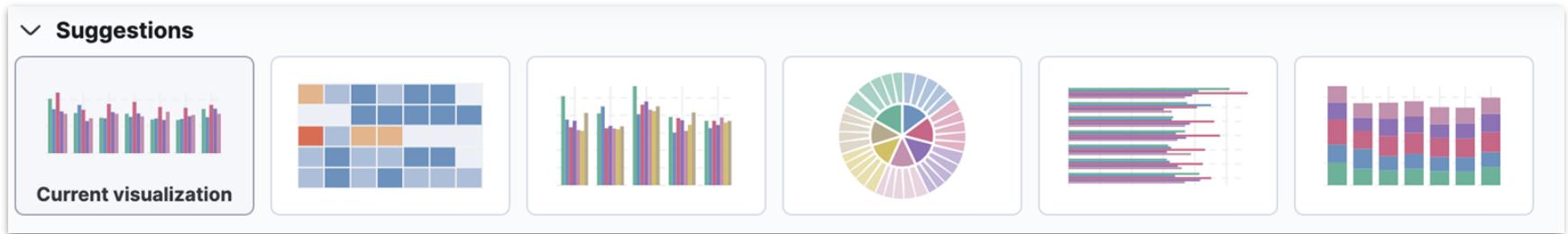
Average	Minimum
Count	Moving average
Counter rate	Percentile
Cumulative sum	Percentile rank
Differences	Standard deviation
Last value	Sum
Maximum	Unique count
Median	

Field

taxful\_total\_price | 

# Suggestions

- Based on selected fields
- Automatically created
- Collapsible



# Contextual configuration options

- A change in one panel will impact the other panes
  - using a **Suggestion** updates the workspace and layers pane
  - changing the **visualization type** in the workspace changes the suggestions and layers pane
  - changes in the **layers pane** are immediately visible in the workspace
- **Quick functions** in the layers pane are driven by the data type
  - some functions are not available for certain types

# Summary: Create visualizations

Module 3 Lesson 1

# Summary

- Lens is the default editor for creating visualizations
  - contains the workspace, fields list, and layers pane
- Visualize data in many different ways
  - bar, line, area graphs
  - pie, donut, treemap charts
  - heatmaps
- Different visualization types have different sets of field groups
  - can be customized with different color schemes, display names and number formats
- Math and grouping functions can be used to display complex data

# Quiz

1. **True or False:** You cannot switch between a pie chart and a bar graph because they do not share the same field groups
2. What would be a good visualization type to show proportional data?
3. Where would you find the control for the number of values to show in a top values graph: the **layer pane**, **workspace**, or **fields list**?

# Create visualizations

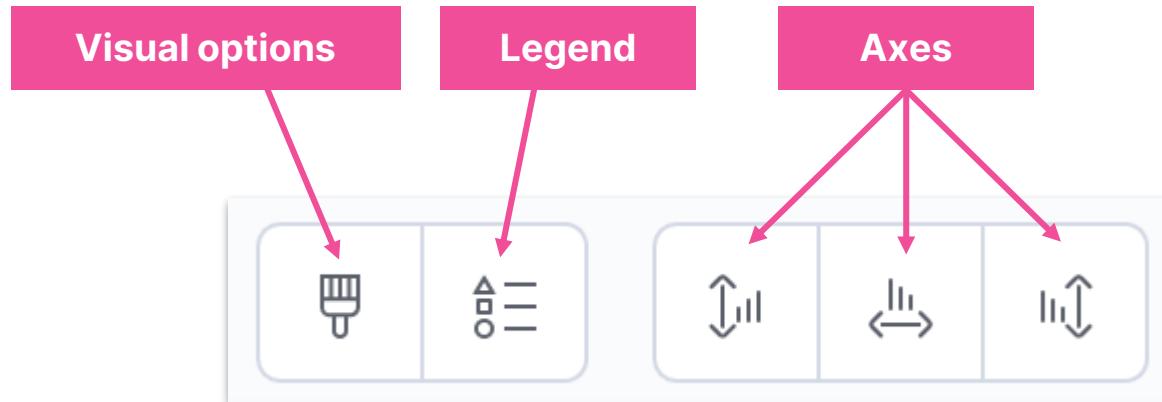
Lab 3.1 - Build visualizations with Lens

# Adjust visualizations

Module 3 Lesson 2

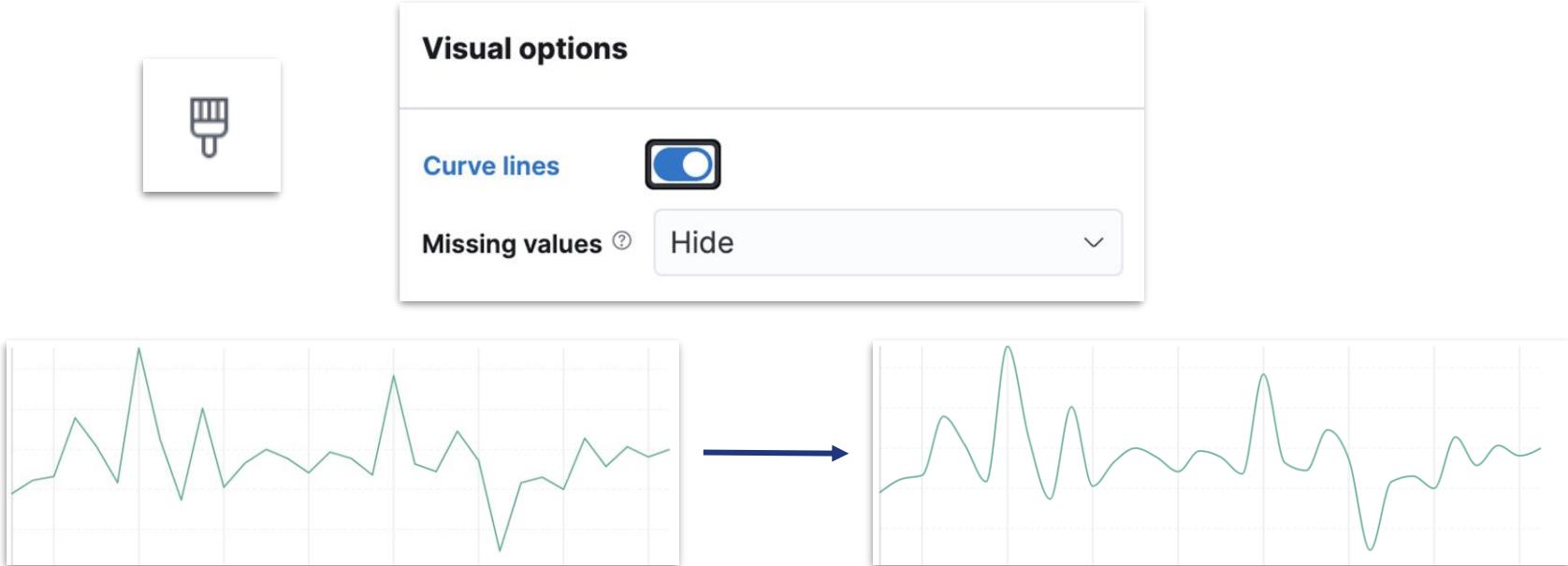
# Visualization options

- There are several ways to adjust the look of your visualizations



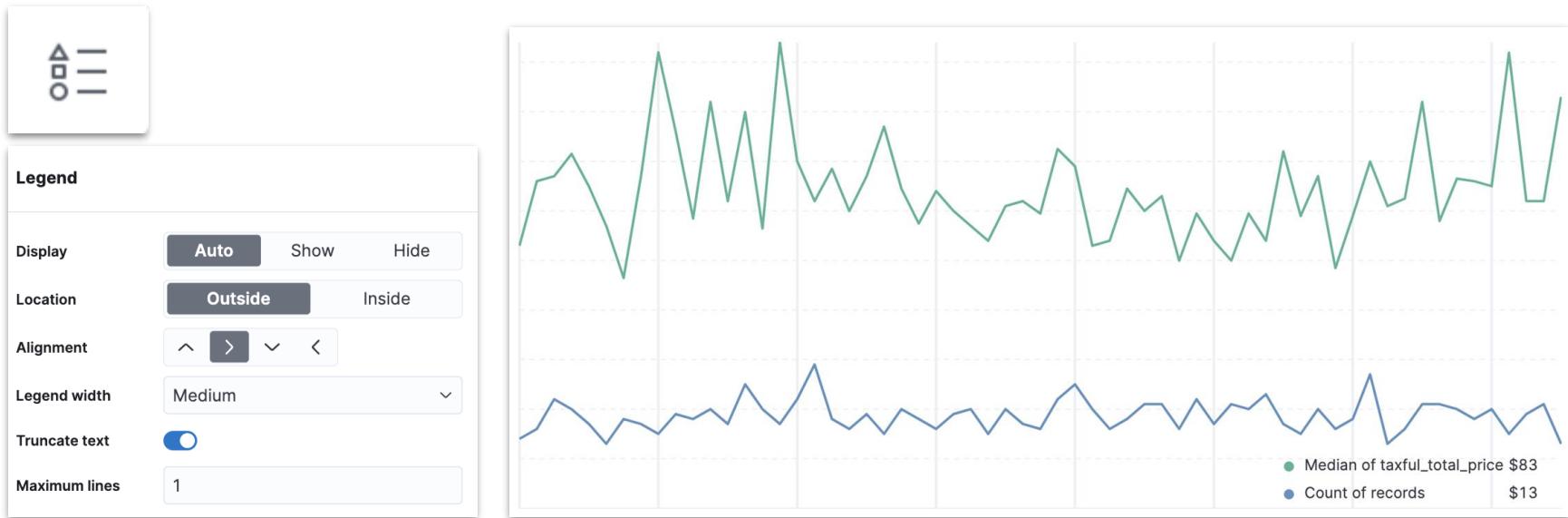
# Visual options

- For the **line** visualization type, you will have the option to draw a smooth curve



# Legend

- Options for the placement and look of your legend



# Left and right axes

- Adjust vertical axis bounds using left and right axis options
- Vertical axes can be separated and options can be applied separately



# Vertical axis bounds



# Bottom axis

- Change axes labels, tick labels, and tick label orientation



# Value format

- Change the way the ticks values are displayed

Appearance

Name Median of taxful\_total\_price

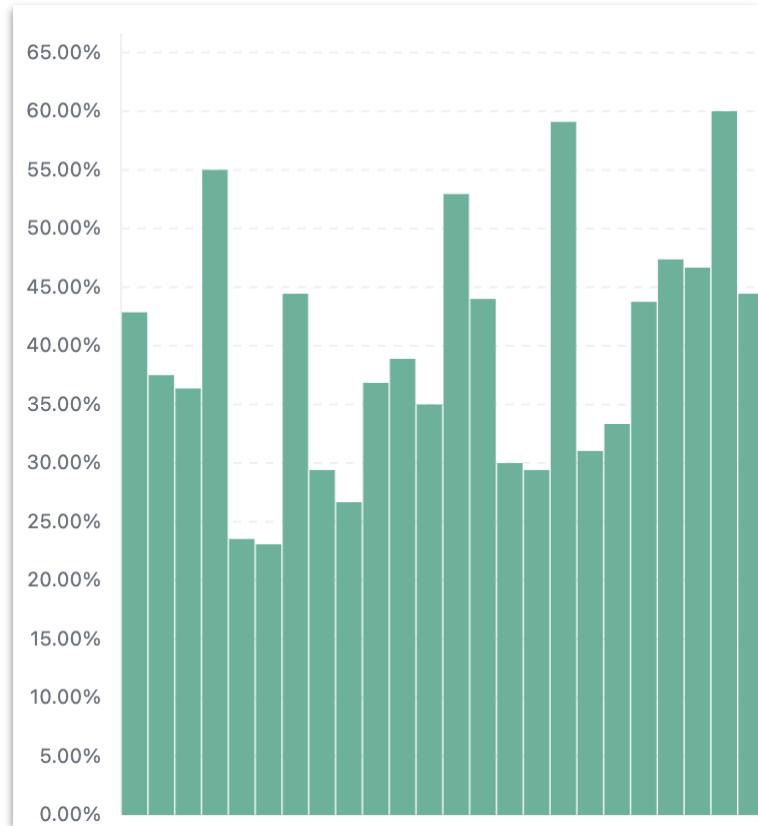
**Value format** Percent

Decimals 2

Suffix

Series color  Auto

Axis side Left **Auto** Right



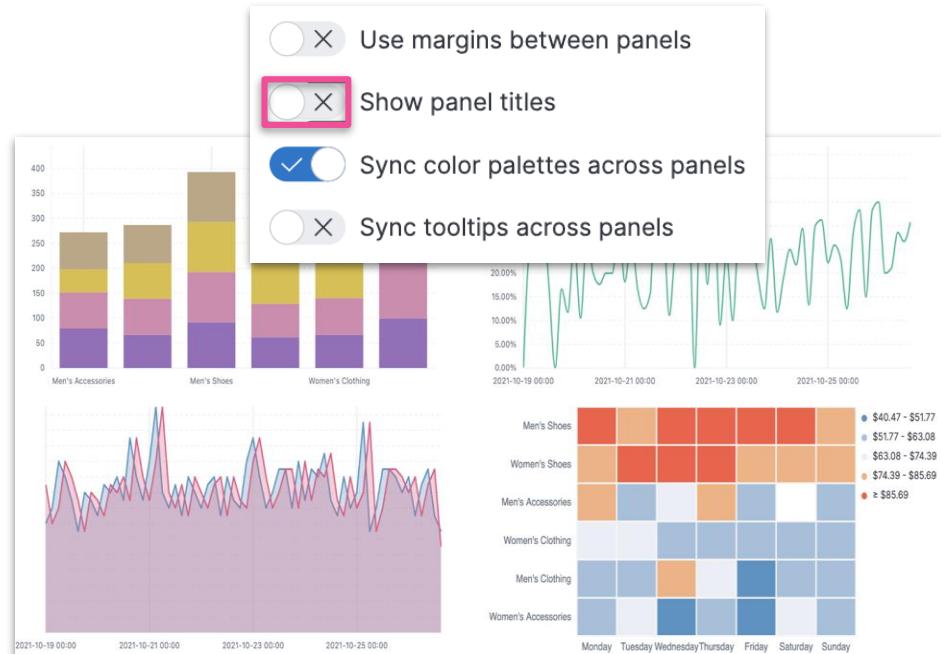
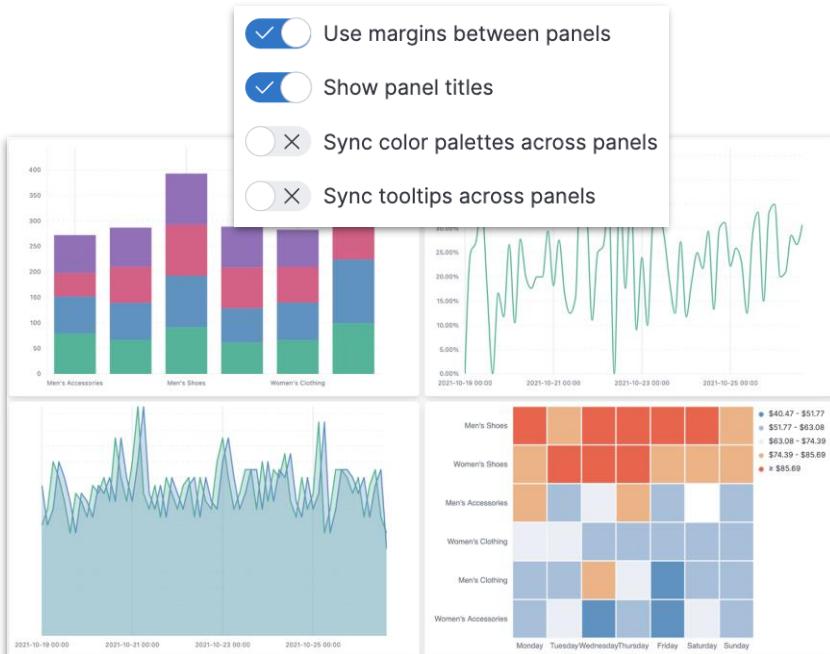
# Time shift

- If the horizontal axis uses a date type field, you can set a time shift factor to compare graphs over a fixed time interval



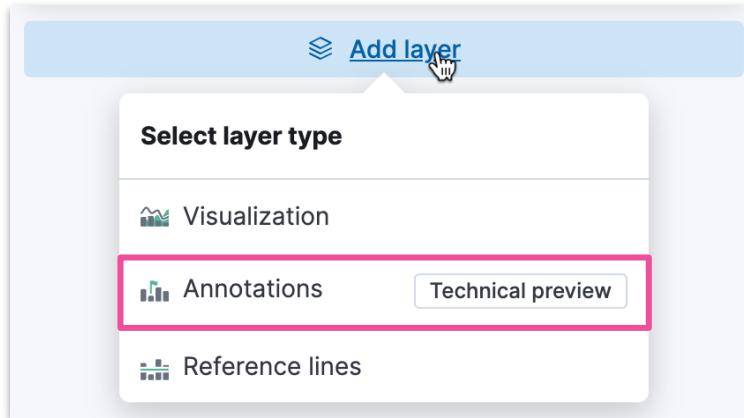
# Dashboard options

- Change how visualizations are displayed on dashboards



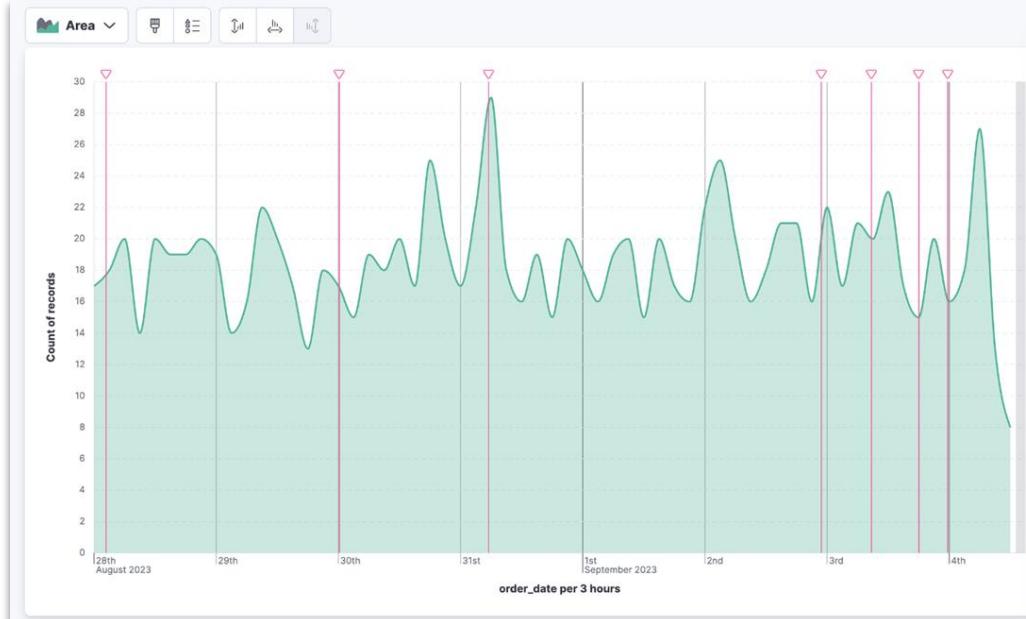
# Annotations

- Annotations are used call out significant changes and trends in your time-based visualizations
  - can also incorporate all of your global filters
- Specified by adding a layer to a visualization



# Creating an annotation

- **Static annotation** - directly specify
- **Custom query** - query using KQL



Horizontal axis annotation

Placement

Placement type

Static date  Custom query

Annotation query

manufacturer.keyword: "Crystal Lighting"

Target date field

order\_date

Appearance

Name Event

Icon decoration ▾ Triangle

Text decoration None

Line 1 px

Color #F04E98

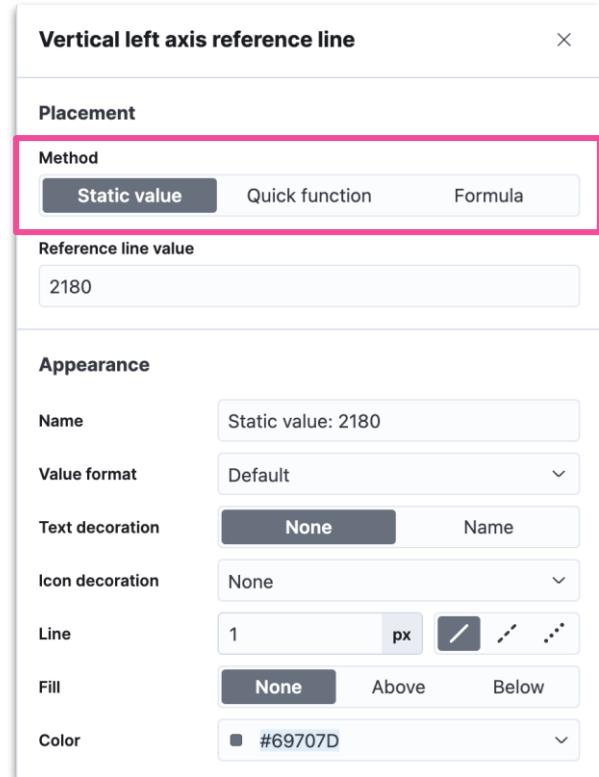
Hide annotation

Tooltip

Show additional fields

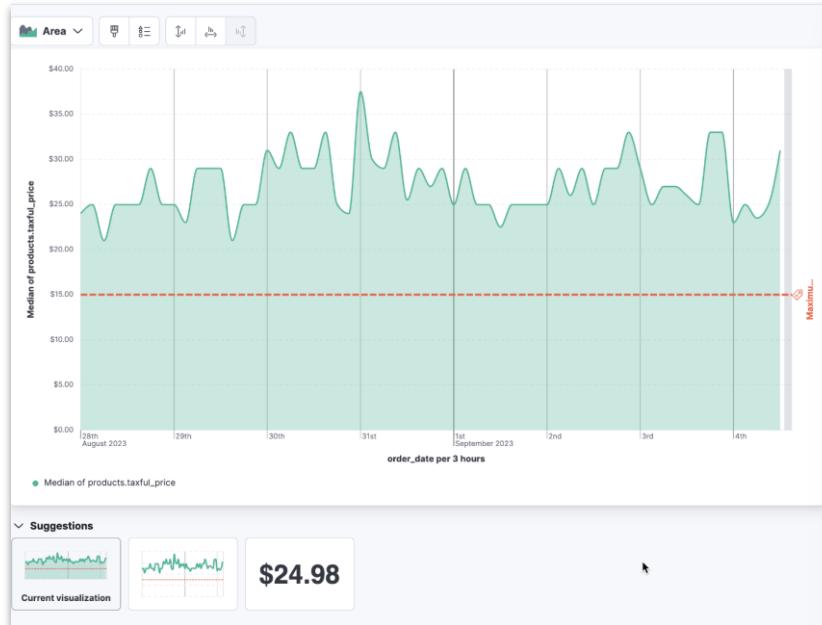
# Reference lines

- Specified by adding a layer to a visualization
- Three types:
  - **Static** - directly specify
  - **Quick function** - select the field and relevant quick function
  - **Formula** - create the custom mathematical formula to apply



# Using Quick functions for reference lines

- Select the function and field to apply for the reference line



Vertical left axis reference line

Functions

- Average
- Count
- Counter rate
- Cumulative sum
- Differences
- Last value
- Maximum (selected)
- Minimum
- Moving average
- Percentile
- Percentile rank
- Standard deviation
- Sum
- Unique count
- Median

Field

products.discount\_amount

Advanced

Appearance

Name: Maximum of products.discount\_amou

Value format: Default

Text decoration: None Name

Icon decoration: Tag

Decoration position: Left Auto Right

Line: 3 px

Fill: None Above Below

# Summary: Adjust visualizations

Module 3 Lesson 2

# Summary

- Show, hide, and adjust **labels, ticks, axes, legends** on your Lens visualization
- Change the **bounds** of your vertical axes to reveal more details in your chart
- Time series charts can be displayed with a **time shift**
- Use **annotations** and **reference lines** to highlight specific events

# Quiz

1. **True or False:** Adjusting the look of a visualization may help to reveal information that could have been otherwise obscured
2. What could be a good way to visualize how your daily sales revenue compares week to week?
3. **True or False:** To hide all panel titles on a dashboard, you have to hide the panel title for each panel separately

# Adjust visualizations

Lab 3.2 - Improve Logs visualizations

# Create maps

Module 3 Lesson 3

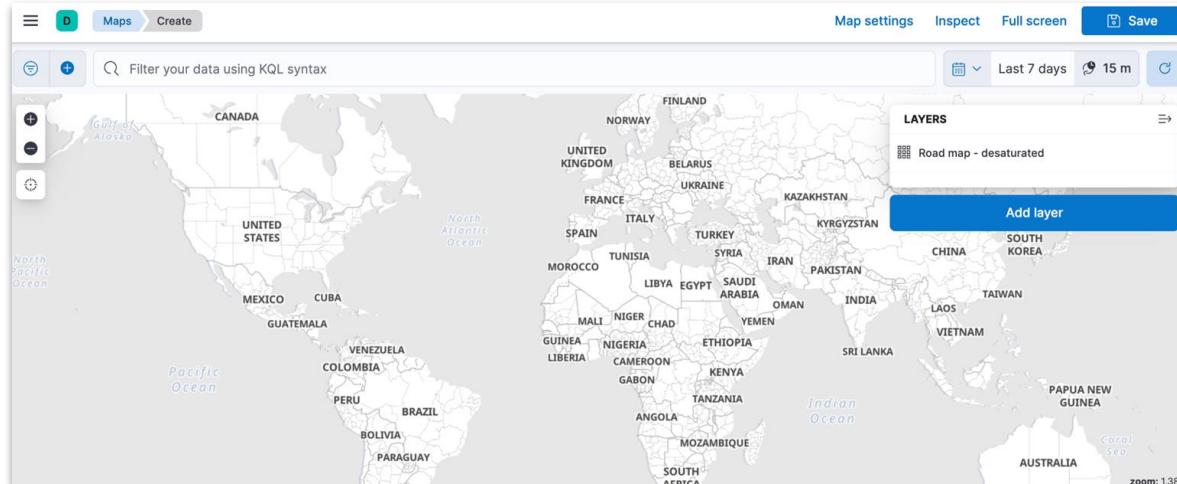
# Maps

- Maps from geographical data
- Animate data
  - temporal + spatial
- Upload
  - GeoJSON
  - shape files

 <b>Documents</b> Points, lines and polygons from Elasticsearch	 <b>Choropleth</b> Shaded areas to compare statistics across boundaries
 <b>Clusters</b> Group Elasticsearch documents into grids and hexagons and display metrics for each group	 <b>Heat map</b> Geospatial data grouped in grids to show density
 <b>Top hits per entity</b> Display the most relevant documents per entity, e.g. the most recent GPS hits per vehicle.	 <b>Tracks</b> Create lines from points
 <b>Point to point</b> Aggregated data paths between the source and destination	 <b>Create index</b> Draw shapes on the map and index in Elasticsearch

# Map layers

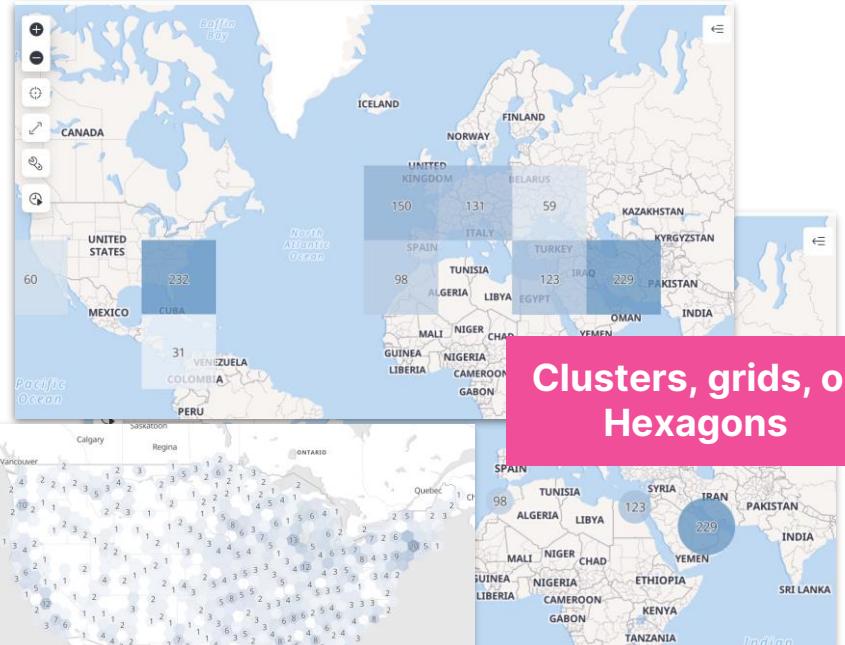
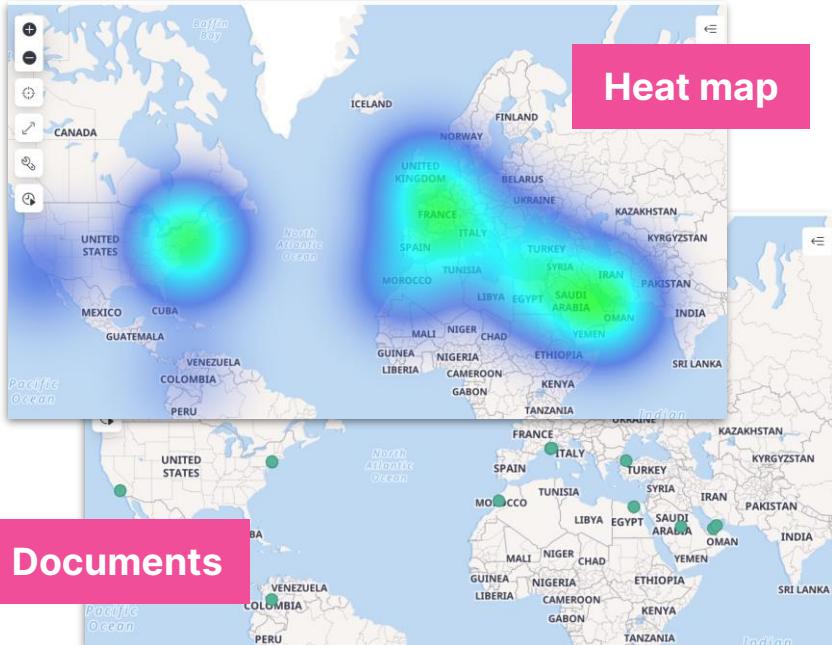
- Maps start with a world Basemap layer
- Add multiple layers
  - from multiple sources
  - Elasticsearch indices



© Copyright Elasticsearch BV 2015-2024 Copying, publishing and/or distributing without written permission is strictly prohibited

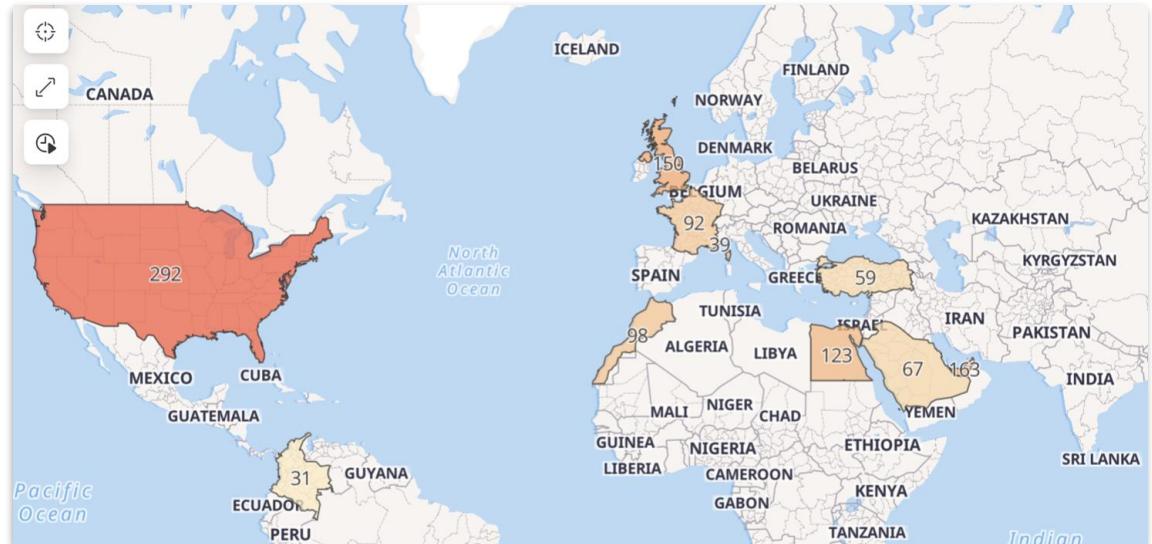
# Plotting data

- Plot individual documents or use aggregations



# Choropleth

- Uses Shading
  - to compare statistics
  - across geographic boundaries



# Boundaries source

- Elastic Maps Service (EMS)
  - [maps.elastic.co](https://maps.elastic.co)
  - Join field
    - format must match source
- Elasticsearch indices

**Boundaries source**

Administrative boundaries from the Elastic Maps Service  
 Points, lines, and polygons from Elasticsearch

**EMS boundaries**

World Countries ▾

**Join field**

ISO 3166-1 alpha-2 code ▾

**Statistics source**

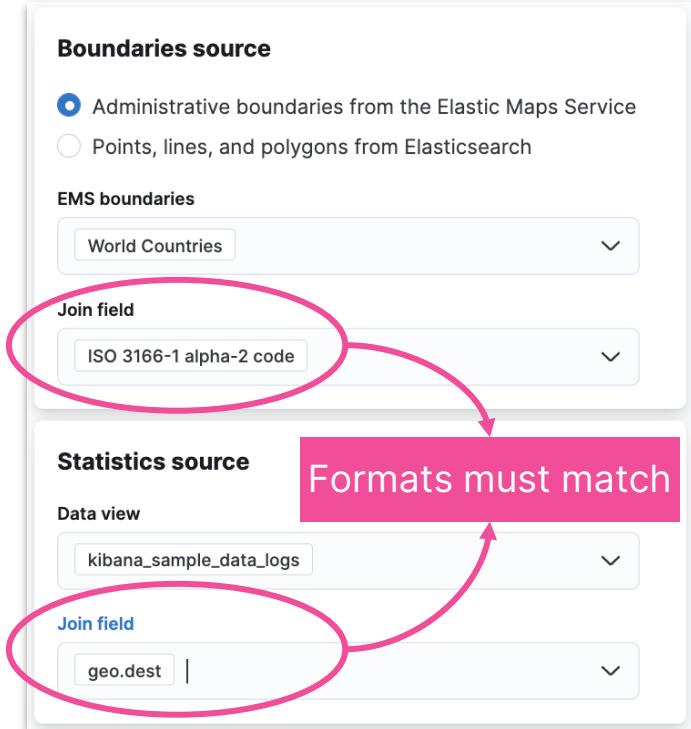
Forms must match

Data view

kibana\_sample\_data\_logs ▾

**Join field**

geo.dest | ▾



ISO 3166-1 alpha-2 code (iso2)	ISO 3166-1 alpha-3 code (iso3)	ISO 3166-1 numeric code (iso_numeric)	name (name)
AD	AND	020	Andorra
AE	ARE	784	United Arab Emirates
AF	AFG	004	Afghanistan

# Point to point

- Data paths between the source and the destination
- Thicker / darker  $\Leftrightarrow$  more connections
- Use cases
  - network traffic
  - flight connections
  - import / export
  - pick-up / drop-off



# Settings & Style

- Layer settings
- Metrics
- Clusters
- Filtering
- Layer Style

**Layer settings**

Name:

Visibility: Zoom levels 0 → 24

Opacity: 75%

Include layer in fit to data bounds computation

Show tooltips

**Tooltip fields**

ISO 3166-1 alpha-2 code

Add

**Term joins** ?

Join World Countries:iso2 with Kibana Sample Data Logs:geo.dest

and use metric count where -- add filter --

Apply global search to join

Apply global time to join

Add join

**Layer style**

**Fill color**

By value: count of Kibana Sample Data Logs

As number:

Reverse colors

**Border color**

Solid: #3D3D3D

**Border width**

Fixed: 1 px

**Label**

By value: count of Kibana Sample Data Logs

**Label visibility**

Use layer visibility

**Label color**

Solid: #000000

**Label size**

Fixed: 14 px

**Label border color**

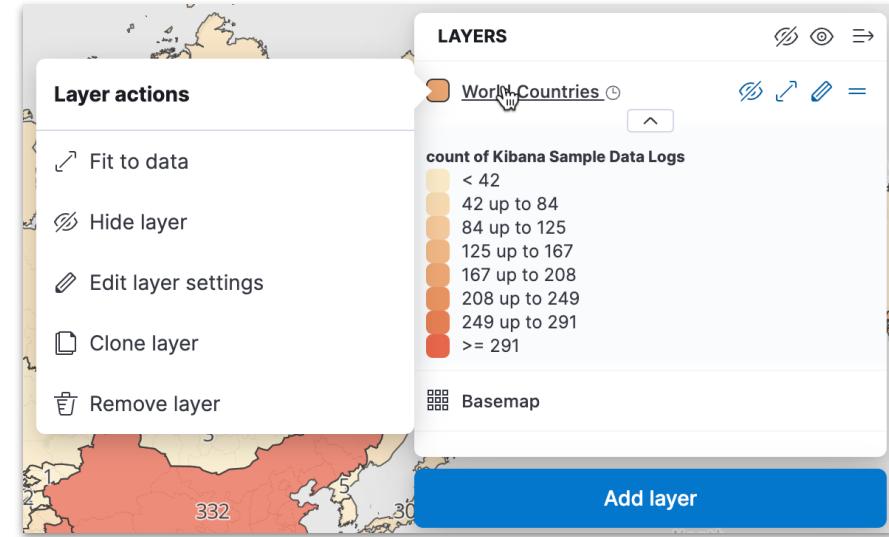
Solid: #FFFFFF

**Label border width**

Small

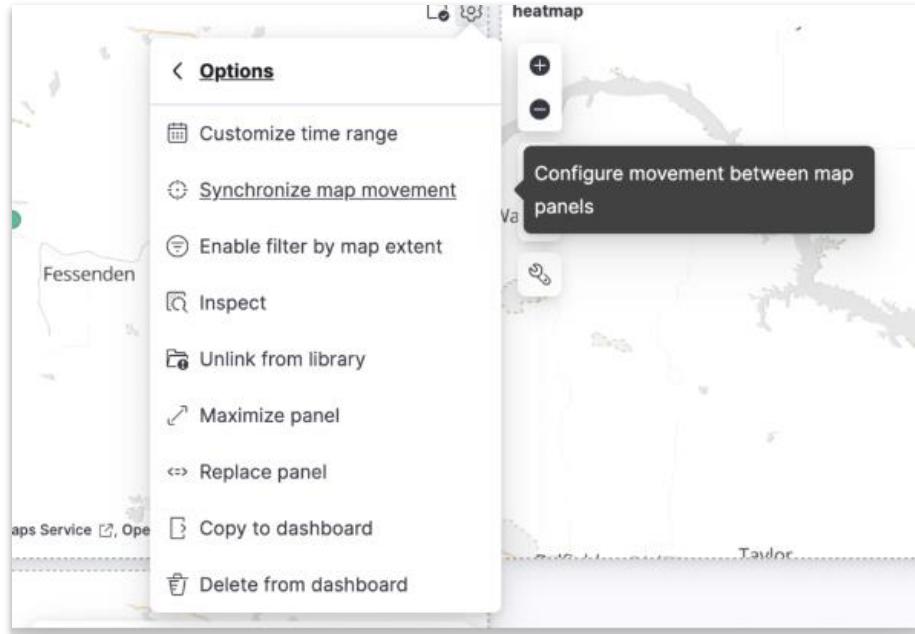
# Managing layers

- After a layer is created, it can be manipulated
  - **Fit to data** zooms the map
  - **Hide layer**
  - **Edit layer settings** to make changes
  - **Clone layer** makes a copy
  - **Remove layer**
- Can also organize layers into **groups**



# Synchronize maps on a dashboard

- Zoom or move in one map and all maps move together



# Summary: Create maps

Module 3 Lesson 3

# Summary

- Maps can use geospatial fields to display records
- Maps can join keywords to regional data
- Multiple map types may be used in a single visualization
  - and each layer can be hidden, cloned, edited, removed or fit
- Each map has colors, tooltips and labels that can be customized

# Quiz

1. **True or False:** A choropleth displays regional boundaries
2. How many geopoint fields must be available in a document for a Point to Point map?
3. Name three actions that can be taken on a layer.

# Create maps

Lab 3.3 - Build Maps from the Logs data

# Data Analysis with Kibana: Agenda

- Getting Started
- Search your Data
- Visualize your Data
- **Additional Visualizations**
- Present your Data
- Analyze your Data with Machine Learning
- Advanced Kibana
- Alerting

# Additional Visualizations

Module 4

# Lessons

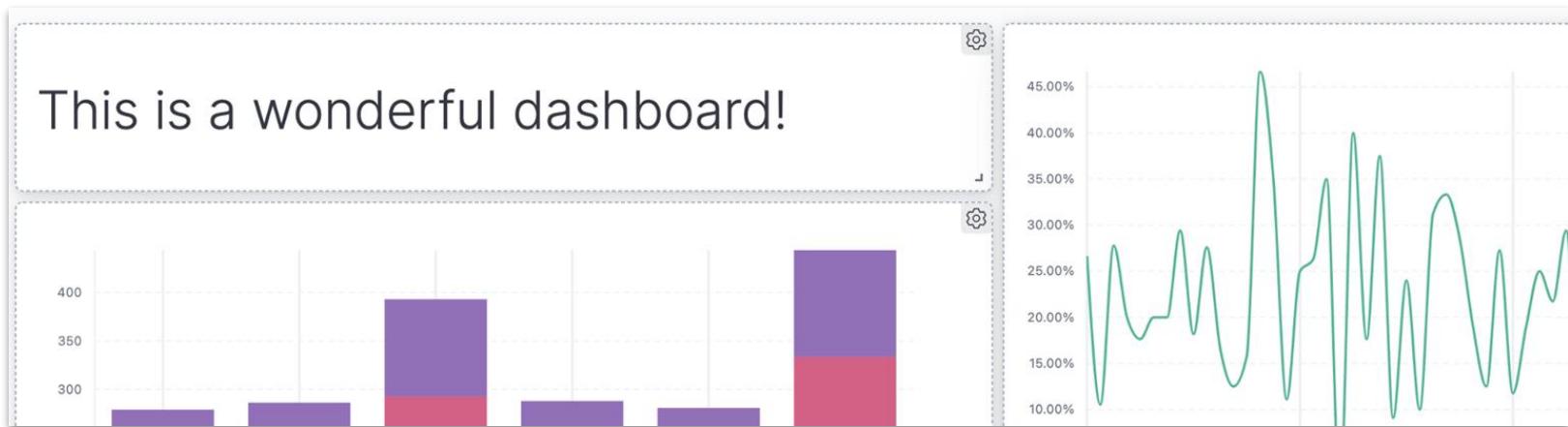
- Text and metrics
- Tables
- Interactive dashboards

# Text and metrics

Module 4 Lesson 1

# Text on dashboards

- Text can help to
  - display values
  - describe visualizations
  - navigate to other dashboards
  - brand dashboards
  - add images
  - provide instructions



# Adding text panels

- Add Markdown text as a **Text** panel
  - on the dashboard, click the text icon
  - in the **Markdown** field,  
enter the markdown
  - click **Update** to see a preview

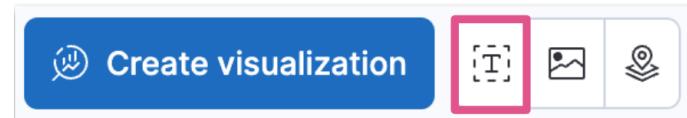
Uses GitHub-flavored  
Markdown text

Data Options

**Markdown**

```
### More on modules

- [Metricbeat modules](https://www.elastic.co/guide/en/beats/metricbeat/7.17/appendix-modules.html)
- [Filebeat modules](https://www.elastic.co/guide/en/beats/filebeat/current/appendix-modules.html)
```



Can also  
Select type > Text

Looks like

More on modules

- [Metricbeat modules](#)
- [Filebeat modules](#)

# Markdown help

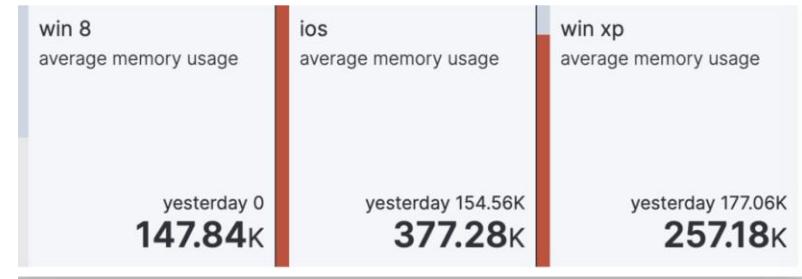
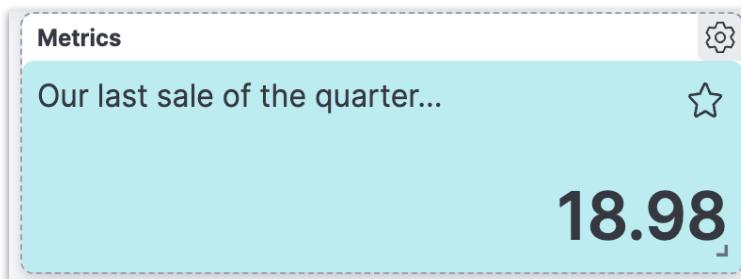
- Click **Help** to access GitHub Docs: <https://docs.github.com/en/get-started/writing-on-github>

The screenshot shows the GitHub Docs interface with the URL <https://docs.github.com/en/get-started/writing-on-github>. The left sidebar has a 'Get started' section with various links like Quickstart, Onboarding, Learning about GitHub, Signing up for GitHub, Using GitHub, Writing on GitHub, Start writing on GitHub, Quickstart, About writing & formatting, Basic formatting syntax (which is selected), Work with advanced formatting, Work with saved replies, and Share content with gists. The main content area is titled 'Styling text' and contains a table comparing different styling methods (Style, Syntax, Keyboard shortcut, Example, Output) for Bold, Italic, Strikethrough, and Bold and nested italic.

Style	Syntax	Keyboard shortcut	Example	Output
Bold	<code>** **</code> or <code>-- --</code>	Command + B (Mac) or Ctrl + B (Windows/Linux)	<code>**This is bold text**</code>	This is bold text
Italic	<code>* * or _</code>	Command + I (Mac) or Ctrl + I (Windows/Linux)	<code>_This text is italicized_</code>	This text is italicized
Strikethrough	<code>~~ ~~</code>	None	<code>~~This was mistaken text~~</code>	This was mistaken text
Bold and nested italic	<code>** ** and _ _</code>	None	<code>**_<u>This text is extremely important</u>**</code>	This text is extremely important

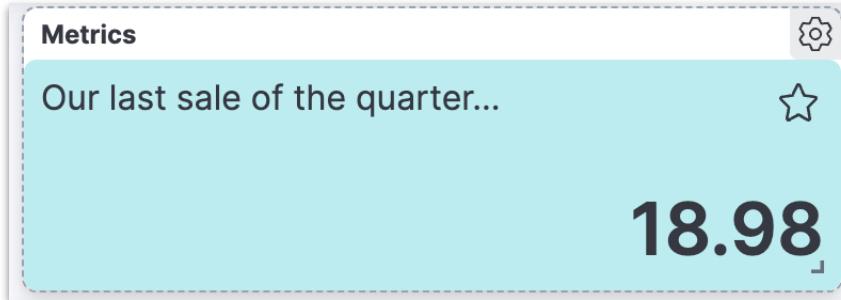
# Metric

- Sometimes a simple view is the best way to display data
  - display a **Primary** metric
  - add an optional **Secondary** metric which can be useful for time shifts and other relevant information
  - for multiple metrics use **Break down** by field to arrange in a grid



# Displaying one panel

- Display one numeric value
  - specify the **Primary metric**
  - use **Quick functions** for basic metrics

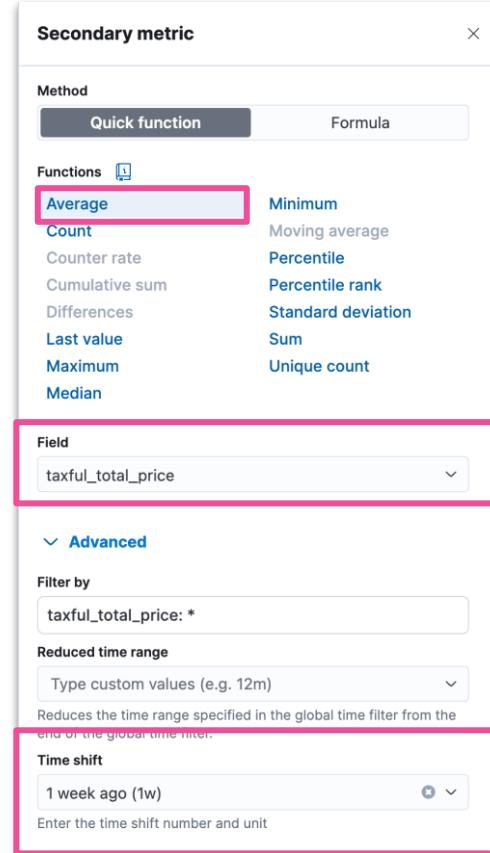


- **Last value** shows the value of the last document (most recent) in the data by date

The screenshot shows the "Primary metric" configuration dialog. It has tabs for "Value" and "Method". The "Method" tab is selected, showing two options: "Quick function" (which is highlighted with a pink border) and "Formula". Under "Quick function", a list of functions is shown, with "Last value" also highlighted with a pink border. Other functions listed include Average, Count, Counter rate, Cumulative sum, Differences, Minimum, Moving average, Percentile, Percentile rank, Standard deviation, Sum, and Unique count. Below the functions, there is a "Field" dropdown set to "taxful\_total\_price", which is also highlighted with a pink border. There is a checkbox for "Show array values" which is unchecked. At the bottom, there is a "Sort by date field" dropdown set to "order\_date", which is also highlighted with a pink border. A link to "Advanced" settings is at the bottom right.

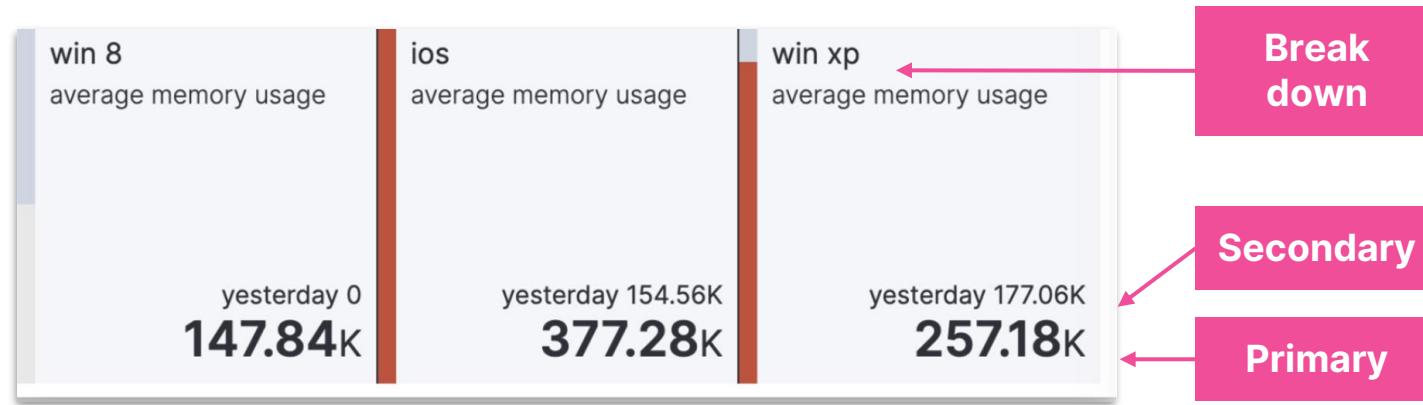
# Adding a Secondary Metric

- Add a Secondary metric
  - can be useful for time shifts or supplementary information



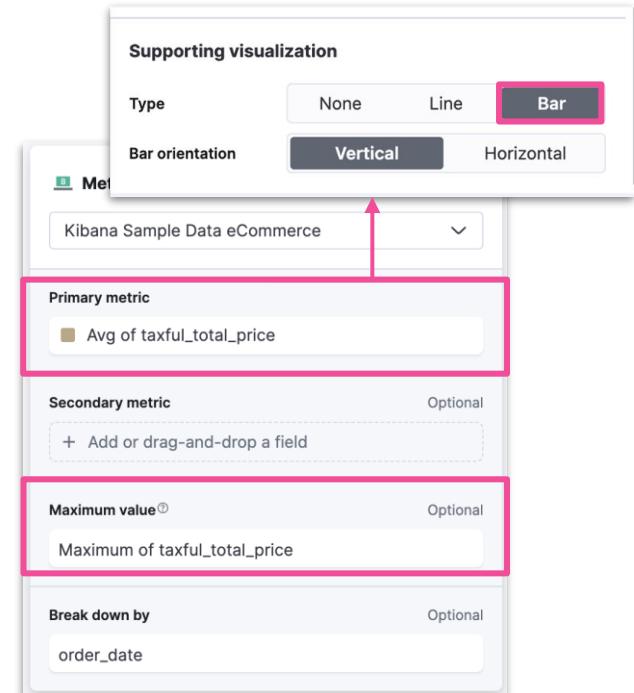
# Displaying multiple metrics

- Use **Break down** by field for multiple metrics arranged in a grid



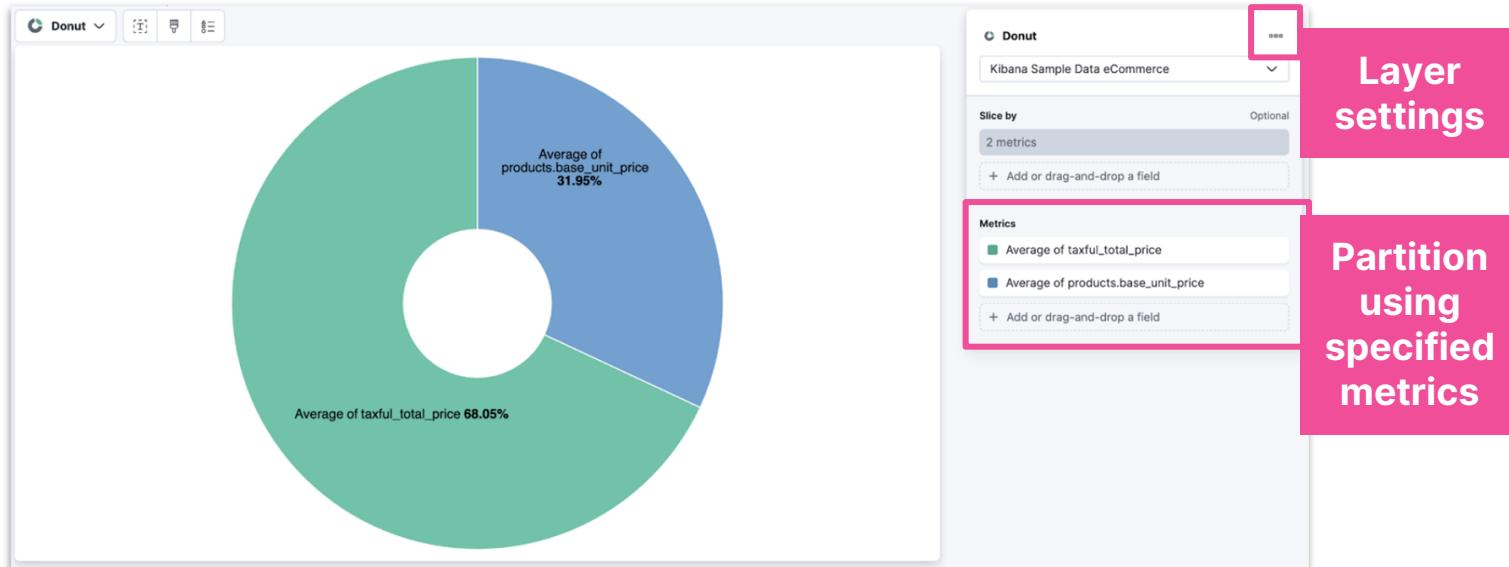
# Supporting Visualization

- Add Line or Bar visualizations to the metric chart
  - defined by **Maximum value**
  - specified in **Primary metric** setting



# Partition charts with multiple metrics

- Enable multiple metrics in layer settings
- Drag and drop two or more fields to partition visualization
- Not a valid option for all chart types



# Summary: Text and metrics

Module 4 Lesson 1

# Summary

- **Text** can add context to dashboard panels
  - add links and images to your dashboards
  - uses GitHub-flavored markdown syntax
- **Metrics** display numerics
  - display supplementary information using a secondary metric
  - use breakdown to show multiple metrics
  - various mathematical formulas may be applied
  - other types of charts, such as pie charts, can be partitioned using metrics

# Quiz

1. Using the **Metrics** visualization, how do you create multiple metrics that are arranged in a grid?
2. How can you use **Text** to navigate between dashboards?
3. What syntax does the Text editor use?

# Text on dashboards

Lab 4.1 - Metrics and Markdown  
visualizations

# Tables

Module 4 Lesson 2

# Tables

- Another way to visualize your data

Table ▾ 

Top 5 values ▾ Friday > Count ▾ Thursday > Count ▾ Sunday > Count ▾ Other > Count ▾

Men's Clothing	76	59	59	260
Women's Clothir	69	65	63	239
Men's Shoes	42	24	29	110
Women's Shoes	36	41	44	135
Women's Access	23	38	24	92
Other	-	1	1	4

Rows are how you group your data

The **cells** have the values of the metric computed for each group

# Rows

- When you drag a string into the workspace  
Lens assumes you want to group your data according to the values of that string field
  - The string field defaults to **Rows**
  - The default **Metrics** is **# Records**

Top 5 values of category.keyword	Count of records
Men's Clothing	454
Women's Clothing	436
Women's Shoes	256
Men's Shoes	205
Women's Accessories	177
Other	6

Drag fields to the **Layer Pane** if you don't like the default behavior

The screenshot shows the Kibana Layer Pane configuration for a 'Table' visualization. The 'Rows' section is set to 'Top 5 values of category.keyword'. The 'Metrics' section is set to 'Count of records'. A pink box highlights the 'Rows' section, and another pink box highlights the 'Metrics' section. A callout at the bottom right says 'Click in the Layer Pane to add fields directly'.

Table

Kibana Sample Data eCommerce

Rows Optional

Top 5 values of category.keyword

+ Add or drag-and-drop a field

Split metrics by Optional

+ Add or drag-and-drop a field

Metrics

Count of records

Click in the Layer Pane to add fields directly

# Groups and subgroups

- Drag another string field and Lens will subdivide the groupings

Notice that **Men's Clothing** is repeated for each **day\_of\_week**

Top 5 values of category	Top 3 values of day_of_w	Count of records
Men's Clothing	Friday	76
Men's Clothing	Wednesday	71
Men's Clothing	Saturday	64
Men's Clothing	Other	243
		69
		69
Women's Clothing	Thursday	65
Women's Clothing	Other	233
Women's Shoes	Sunday	44
Women's Shoes	Thursday	11

Table

Kibana Sample Data eCommerce

Rows Optional

Top 5 values of category.keyword

Top 3 values of day\_of\_week

+ Add or drag-and-drop a field

Split metrics by Optional

+ Add or drag-and-drop a field

Metrics

Count of records

+ Add or drag-and-drop a field

# Pivot table

- Use **Split metrics by** to pivot the table

Move `day_of_week` from Rows to **Split metrics by**

The visualization shows a table with the following data:

	Friday	Thursday	Sunday	Other
Men's Clothing	76	59	59	260
Women's Clothir	69	65	63	239
Men's Shoes	42	24	29	110
Women's Shoes	36	41	44	135
Women's Acces:	23	38	24	92
Other	-	1	1	4

The configuration interface shows the following settings:

- Rows**: Top 5 values of category.keyword (Optional)
- Split metrics by**: Top 3 values of day\_of\_week (Optional)
- Metrics**: Count of records

# Metrics

- When you drag a numeric field into an empty Table workspace Lens will group by timestamp
  - The timestamp field defaults to **Rows**
  - The default **Metrics** is **Median**

Table

order_date per 3 hours	Median of taxful_total_price
2023-09-26 15:00	\$79
2023-09-26 18:00	\$53.97
2023-09-26 21:00	\$67
2023-09-27 00:00	\$70
2023-09-27 03:00	\$75
2023-09-27 06:00	\$49.97
2023-09-27 09:00	\$61.47
2023-09-27 12:00	\$58.47
2023-09-27 15:00	\$53.97
2023-09-27 18:00	\$77

Table

Kibana Sample Data eCommerce

Rows Optional

order\_date

+ Add or drag-and-drop a field

Split metrics by Optional

+ Add or drag-and-drop a field

Metrics

Median of taxful\_total\_price

+ Add or drag-and-drop a field

The screenshot shows the Kibana Table workspace configuration. The 'Rows' section is set to 'order\_date'. The 'Metrics' section is set to 'Median of taxful\_total\_price'. Both sections have a red box around them, indicating they are the focus of the slide. The 'Split metrics by' section is empty.

# Many metrics

- Keep adding more numeric fields

Table ▾ Rows

order\_date per 3 hour ▾ Median of taxful\_total ▾ Median of taxless\_tot ▾ Median of total\_quant ▾

2023-09-26 15:00	\$84	\$84.00	2
2023-09-26 18:00	\$53.97	\$53.97	2
2023-09-26 21:00	\$67	\$67.00	2
2023-09-27 00:00	\$70	\$70.00	2
2023-09-27 03:00	\$75	\$75.00	2
2023-09-27 06:00	\$49.97	\$49.97	2
2023-09-27 09:00	\$61.47	\$61.47	2
2023-09-27 12:00	\$58.47	\$58.47	2
2023-09-27 15:00	\$53.97	\$53.97	2
2023-09-27 18:00	\$77	\$77.00	2

Table ...

Kibana Sample Data eCommerce

Rows Optional

order\_date

+ Add or drag-and-drop a field

Split metrics by Optional

+ Add or drag-and-drop a field

Metrics

Median of taxful\_total\_price

Median of taxless\_total\_price

Median of total\_quantity

+ Add or drag-and-drop a field

# Summary row

- You can add a summary row

Table ▾

order\_date per 3 hour ▾ Median of taxful\_total ▾ Median of taxless\_tot ▾ Median of total\_quant ▾

2023-09-26 15:00	\$84	\$84.00	2
2023-09-26 18:00	\$53.97	\$53.97	2
2023-09-26 21:00	\$67	\$67.00	2
2023-09-27 00:00	\$70	\$70.00	2
2023-09-27 03:00	\$75	\$75.00	2
2023-09-27 06:00	\$49.97	\$49.97	2
2023-09-27 09:00	\$61.47	\$61.47	2
2023-09-27 12:00	\$58.47	\$58.47	2
2023-09-27 15:00	\$53.97	\$53.97	2

Average: \$66.33   Sum: \$3,780.63   Maximum: 2

## Summary

Summary Row

Maximum

Summary label

Maximum

# Color by value

## ● Conditional coloring by cell or text

Table Filter

order_date per 3 hour	Median of taxful_total	Median of taxless_tot	Median of total_quant
2023-09-26 15:00	\$84	\$84.00	2
2023-09-26 18:00	\$53.97	\$53.97	2
2023-09-26 21:00	\$67	\$67.00	2
2023-09-27 00:00	\$70	\$70.00	2
2023-09-27 03:00	\$75	\$75.00	2
2023-09-27 06:00	\$49.97	\$49.97	2
2023-09-27 09:00	\$61.47	\$61.47	2
2023-09-27 12:00	\$58.47	\$58.47	2
2023-09-27 15:00	\$53.97	\$53.97	2
Average: \$66.33		Sum: \$3,780.63	Maximum: 2

Appearance

Name: Median of taxful\_total\_price

Value format: Default

Text alignment: Left Center Right

Color by value: Cell (selected)

Color palette: Edit

Hide column:

Color: Edit

Use built in color palettes or select your own color scheme

← Color

Color palette:

Value type: Percent

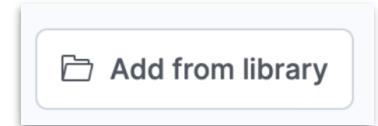
Color Ranges:

- ≥ 0 % MIN
- ≥ 20 %
- ≥ 40 %
- ≥ 60 %
- ≥ 80 %
- ≤ 100 %

Add color Reverse colors Distribute values

# Saved search

- Save a search
- Add it to your dashboard from Visualization library



Taxful Total Price > 100							204 documents
Columns		1 field sorted					
	order_date	category	taxful_total_price	products.price	products.manufacturer	products.sku	
✓	Oct 3, 2023 @ 18:24:29.000	[Men's Clothing, Men's Shoes]	\$190	[\$24.98, \$165.00]	[Elitelligence, (empty)]	[Z00589405894, Z00483304833]	
✓	Oct 3, 2023 @ 17:58:34.000	[Women's Shoes, Women's Clothing]	\$108	[\$75.00, \$33.00]	[Oceanavigations, Gnomehouse]		
✓	Oct 3, 2023 @ 16:43:41.000	[Women's Clothing, Women's Shoes]	\$181	[\$20.98, \$50.00, \$50.00, \$60.00]	[Pyramidustries, Tigress Enterprises, Oceanavigations, Low Tide Media]		
✓	Oct 3, 2023 @ 15:17:17.000	Men's Clothing	\$108	[\$75.00, \$33.00]	[Oceanavigations, Oceanavigations]	[Z00273802738, Z00300303003]	
✓	Oct 3, 2023 @ 14:08:10.000	[Women's Clothing, Women's Shoes]	\$105	[\$29.98, \$75.00]	[Tigress Enterprises, Angeldale]	[Z00039400394, Z00672906729]	

Useful for tables  
created in Discover

# Summary: Tables

Module 4 Lesson 2

# Summary

- Lens allows you to create custom tables
- Tables are highly customizable, and provide you with text alignment, value formatting, coloring options, and more
- Summary rows can be used to display the summary value
- Conditional coloring can be set for cells or text
- Add **document tables** from Discover to dashboards using **Saved Search**

# Quiz

1. **True or False:** A **cell** in a table displays the value of a metric for a grouping of data.
2. **True or False:** Conditional coloring can only be set for texts in a table column.
3. **True or False:** Saved searches are good for adding search results to a dashboard in the form of a document table.

# Tables

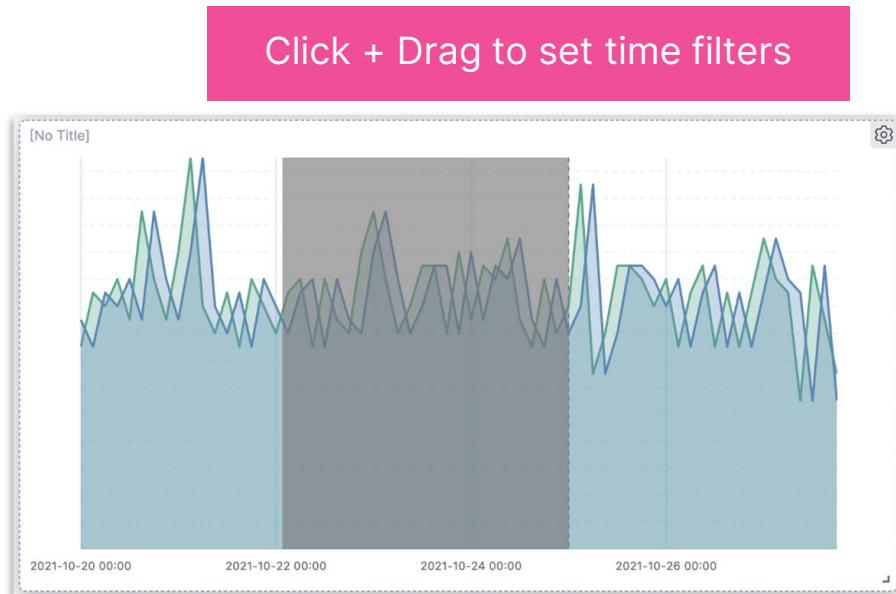
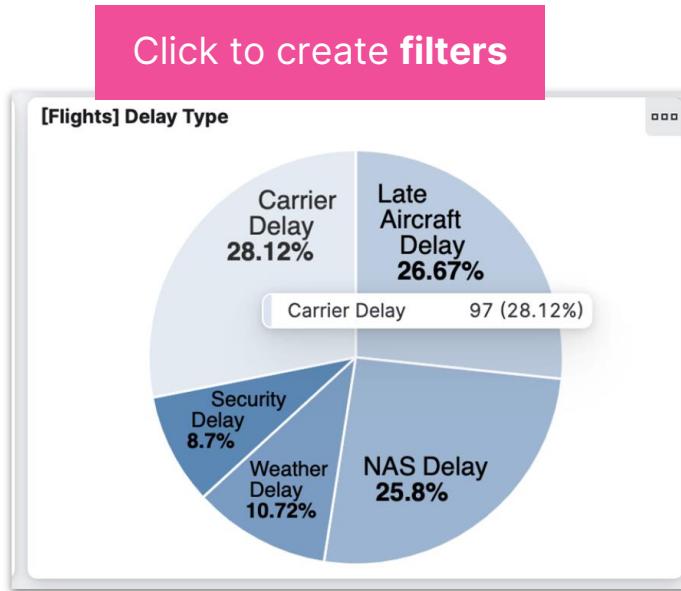
Lab 4.2 - Build a Table with Lens

# Interactive dashboards

Module 4 Lesson 3

# Visualizations can filter data

- Visualizations on your dashboards are interactive



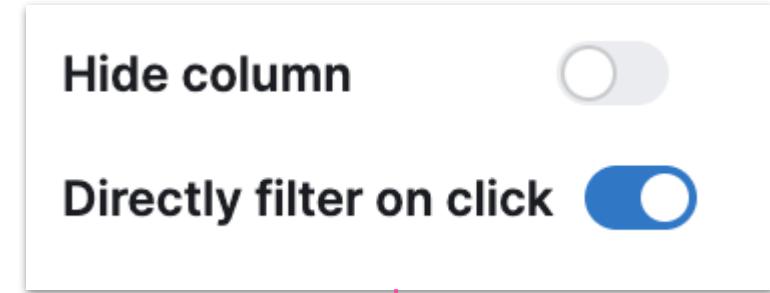
# Tables can filter data

- Click a cell to create a filter
- Optionally enable filter on click

[Flights] Most delayed cities

Top values of OriginCityName

Memphis	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="edit"/>
Memphis	
<input type="button" value="Filter for value"/> <input type="button" value="Filter out value"/>	
Syracuse	



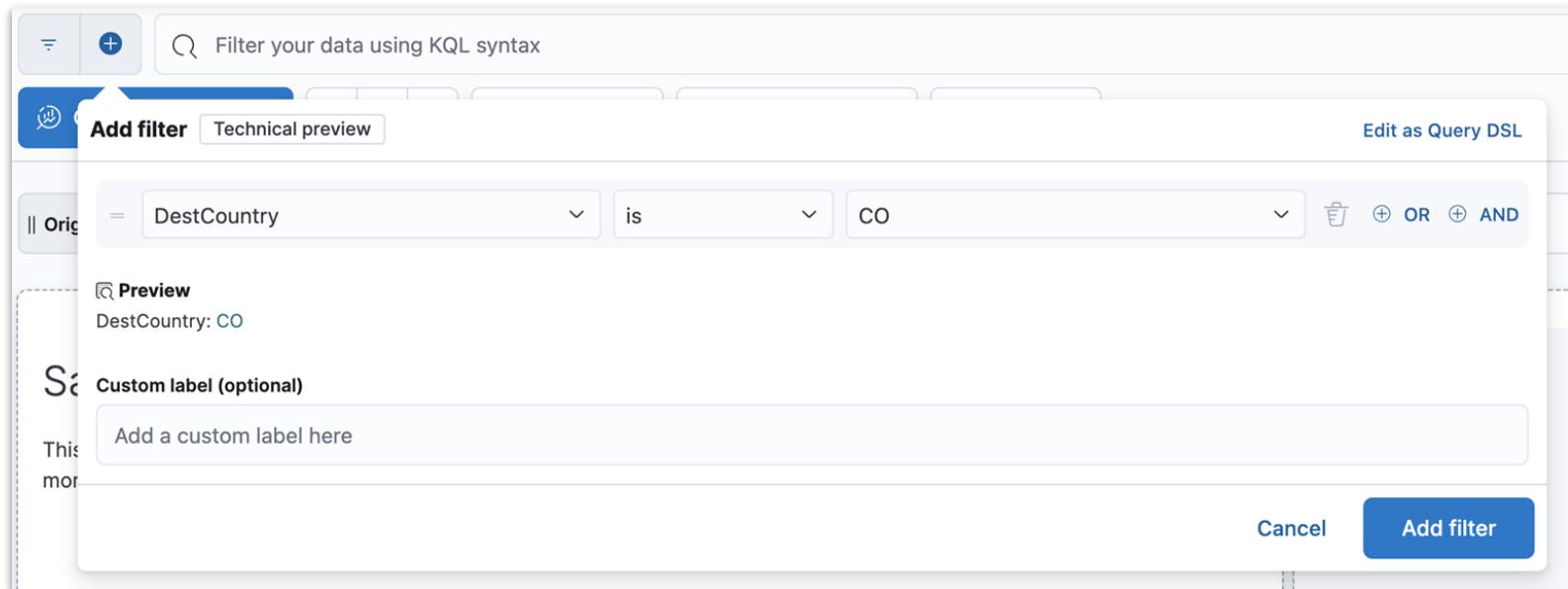
[Flights] Most delayed cities

Top values of OriginCityName

<u>Memphis</u>	<input type="button" value="edit"/>
Raleigh/Durham	
Buffalo	

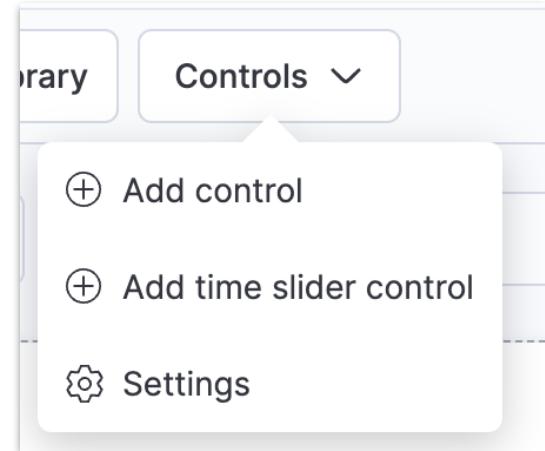
# More filters

- Filters can also be created directly
  - **Add filter** under the query bar



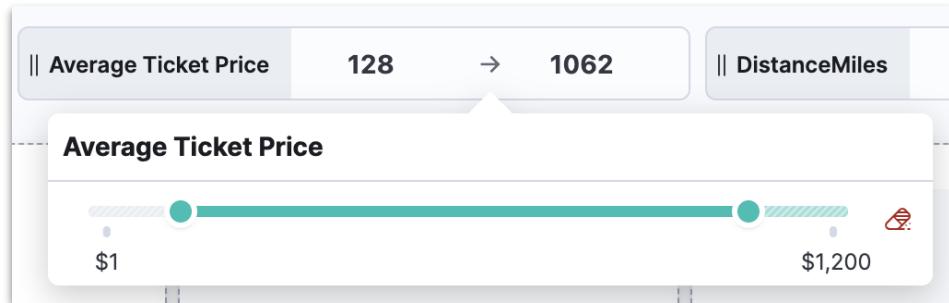
# Controls can filter

- Interactive panes to filter and display only the data you want
- Three types of controls:
  - **Options List:** Dropdown menu with multiple options to select.
  - **Range Slider:** Slider to filter the data within a specified range.
  - **Time Slider:** view the data for a specific time range or playback the data by time



# Range slider

- Select the field you want to create the filter on
- Customize the slider with Label and size

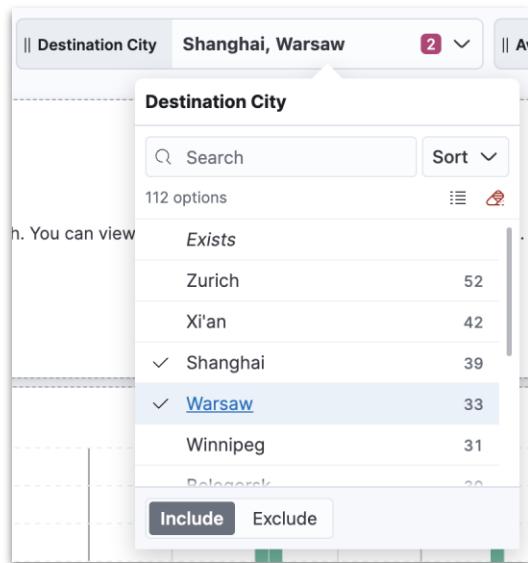


**Field**

 Search field names  
Filter by type 0  
AvgTicketPrice  
Cancelled  
Carrier  
Dest  
DestAirportID  
DestCityName  
DestCountry  
DestRegion  
  
**Control type**  
Range slider  
**Label**  
Average Ticket Price  
**Minimum width**  
Small Medium Large  
 Expand width to fit available space  
  
 Delete control

# Options list

- Allows for multiple selections in the dropdown

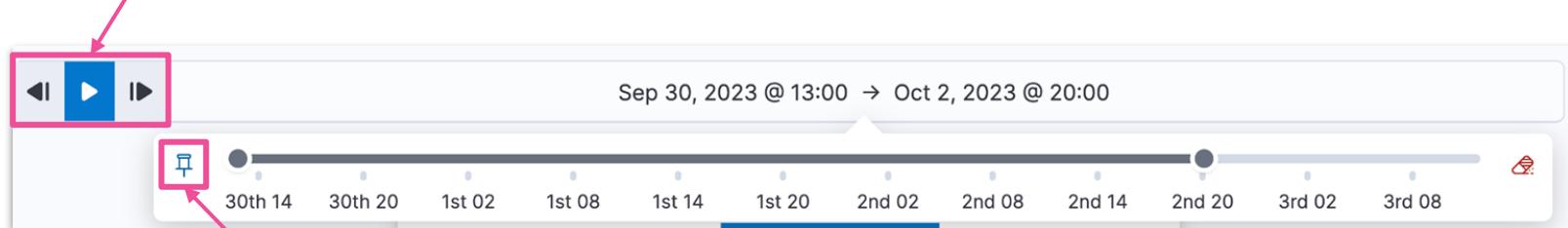


A configuration panel for an "Options list" control. It includes the following sections:

- Control type:** Options list
- Label:** Destination City
- Minimum width:** Small, Medium, Large (Medium is selected)
- Additional settings:**
  - Allow multiple selections in dropdown
  - Ignore timeout for results
- Delete control:** A red "Delete" icon.

# Time slider

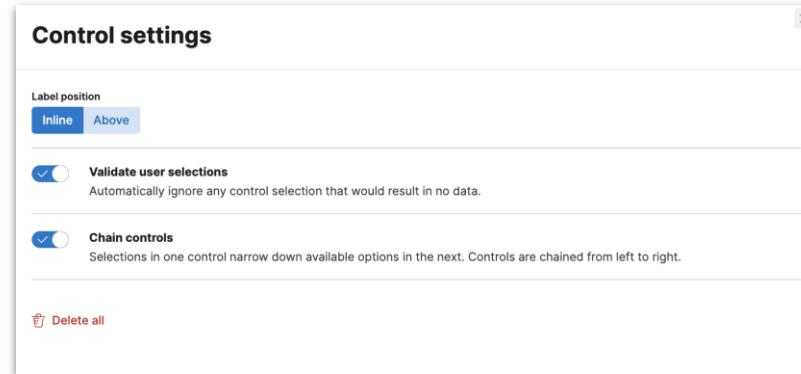
Playback and scrub through the data by time



Pin the start time to show how data builds over a period of time

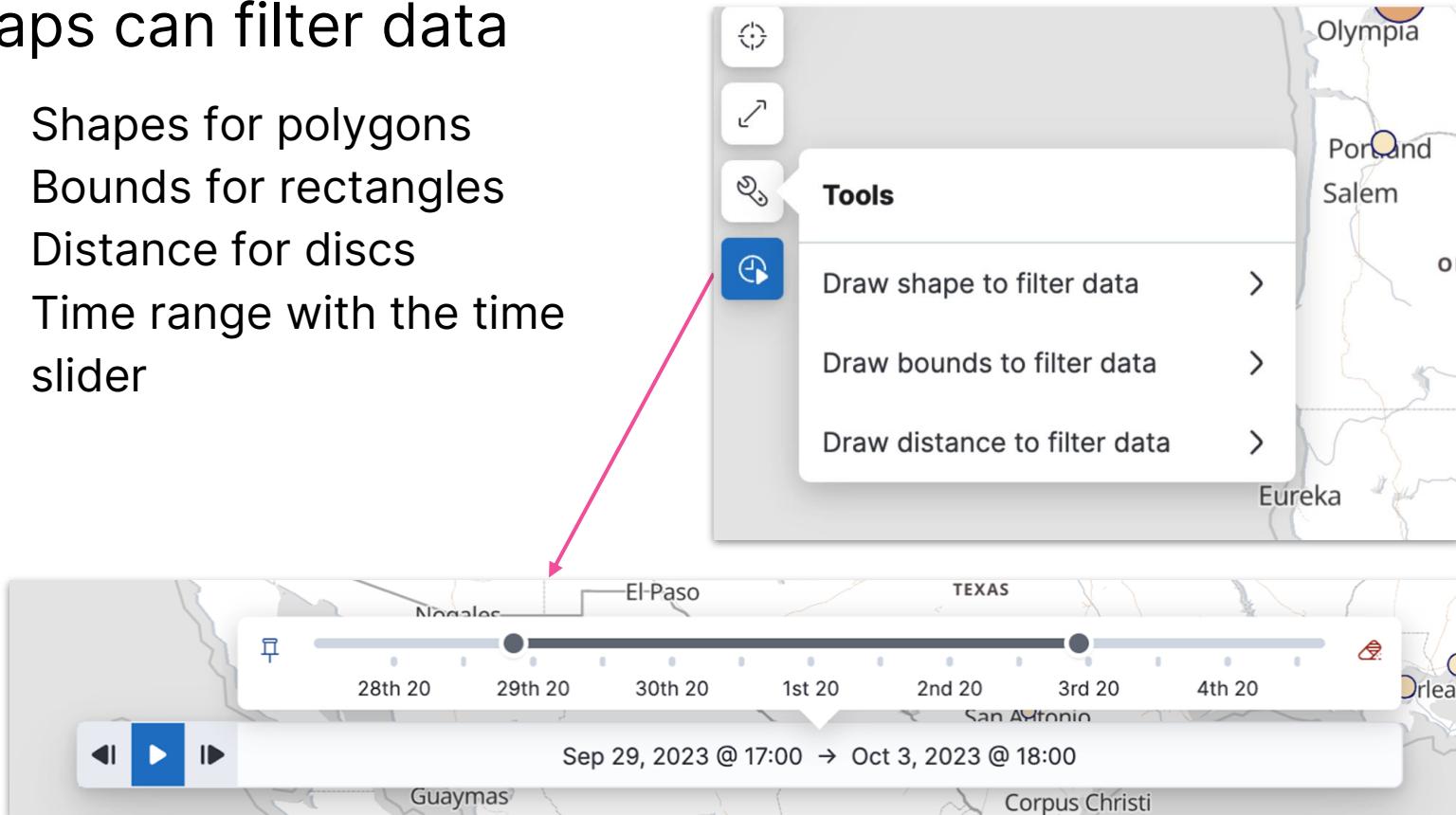
# Control settings

- Multiple settings available for the created controls:
  - **Label position**
  - **Validate user selection:** ignore actions that result in missing data
  - **Chain controls:** any selection in one control narrows the available options in the next control
  - **Delete all controls**



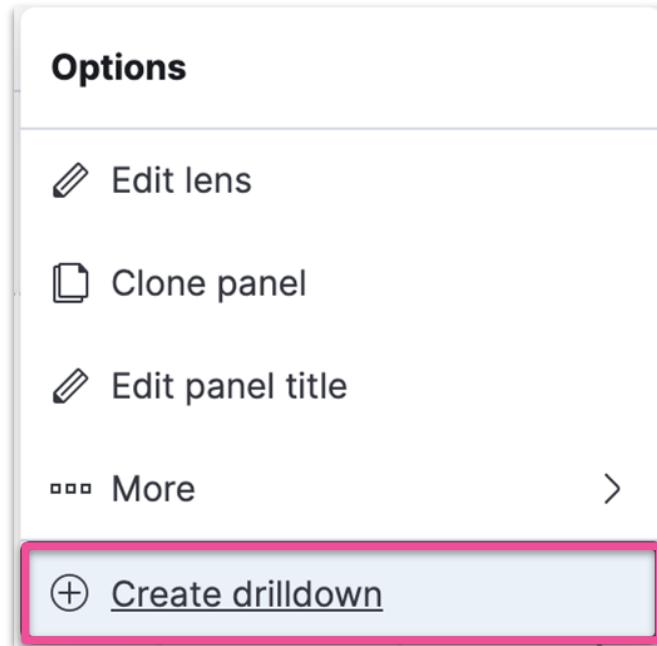
# Maps can filter data

- Shapes for polygons
- Bounds for rectangles
- Distance for discs
- Time range with the time slider



# Drilldowns

- Drilldowns enable you to customize what happens when someone clicks on a value within a dashboard panel



The image shows a white rectangular box with a pink header bar containing the text 'Three types of Drilldowns'. Below the header, there are two tabs: 'Create new' (which is underlined in blue) and 'Manage'. Under 'Create new', there are three items: 'Go to Dashboard' with a dashboard icon, 'Go to URL' with a link icon, and 'Open in Discover' with a magnifying glass icon.

# URL drilldowns

- Create an external link using values from the filter

Name  
Google it!

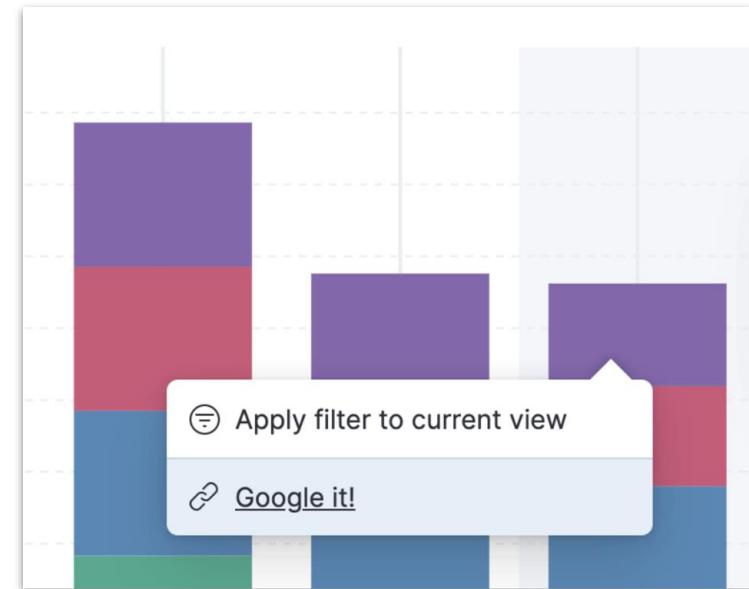
Trigger

**Single click**  
A data point click on the visualization

**Range selection**  
A range of values on the visualization

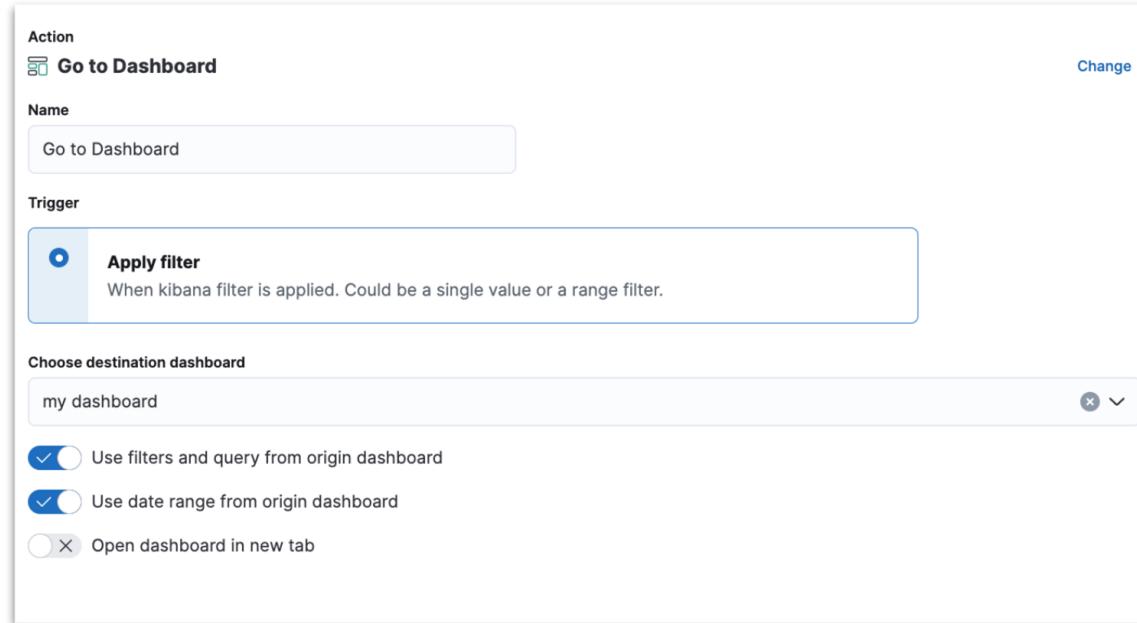
**Context menu**  
A panel top-right corner context menu click.

Enter URL:  
<https://www.google.com/search?q={{event.value}}>



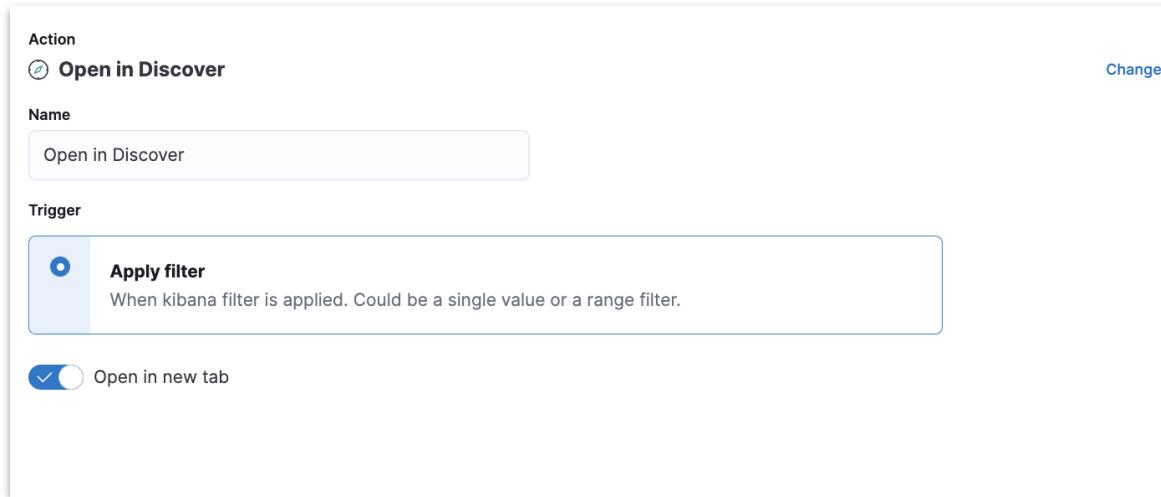
# Dashboard drilldowns

- Or open a new window to a different dashboard with the filters already applied to it



# Discover drilldowns

- Or open a new window to the **Discover** interface with the filter applied from the visualizations



# Summary: Interactive dashboards

Module 4 Lesson 3

# Summary

- Filters can be used to explore your data on your dashboards
- There are many ways to create filters
  - Clicking on a visualization
  - Selecting bounds on a map
  - Add filter menu
  - Setting a control
- Drilldowns can use a filter in other ways, like setting it on another dashboard, or using it in a URL call or in a new discover interface

# Quiz

1. **True or False:** An end user of your dashboard must know about the fields of an index to create a filter.
2. What are the different ways a user can filter data on a dashboard?
3. How can a **Drilldown** be used to drill down your data?

# Interactive dashboards

Lab 4.3 - Controls and Drilldowns features

# Data Analysis with Kibana: Agenda

- Getting Started
- Search your Data
- Visualize your Data
- Additional Visualizations
- **Present your Data**
- Analyze your Data with Machine Learning
- Advanced Kibana
- Alerting

# Present your Data

Module 5

# Lessons

- Sharing a dashboard
- Sharing with users
- Canvas

# Sharing a dashboard

Module 5 Lesson 1

# Share dashboard

- Custom branding
- Using a direct link
- Using an iframe (embedded)
- Generating a report

# Custom branding

The image shows the 'Custom branding' configuration page in the Elasticsearch interface. It includes fields for 'Custom logo', 'Organization name', 'Page title', 'Favicon (SVG)', and 'Favicon (PNG)'. A pink arrow points from the 'Custom logo' field to a screenshot of a browser tab showing a yellow lightbulb icon and the text 'Hello World'. Another pink arrow points from the 'Page title' field to a screenshot of a browser tab showing a yellow lightbulb icon and the text 'The Cool Company'. A third pink arrow points from the 'Favicon (SVG)' field to a screenshot of a browser tab showing a yellow lightbulb icon and the text 'The Cool Company'.

**Custom branding**

**Custom logo**  
Replaces the Elastic logo. Logos look best when they are no larger than 128 × 128 pixels and have a transparent background. Subscription required.  
Default: null

**Organization name**  
Replaces the text next to the logo. Images look best when they are no larger than 200 × 84 pixels and have a transparent background. Subscription required.  
Default: null

**Page title**  
The text that appears on browser tabs. Subscription required.  
Default: null

**Favicon (SVG)**  
The URL of an image that will appear on browser tabs. Recommended size is 16 × 16 pixels. Subscription required.  
Default: null

**Favicon (PNG)**  
The URL of an image for use in browsers that don't support SVG. Subscription required.

xpackCustomBranding.logo  
Reset to default Change image  
xpackCustomBranding.customizedLogo

xpackCustomBranding.pageTitle  
Hello World  
Reset to default

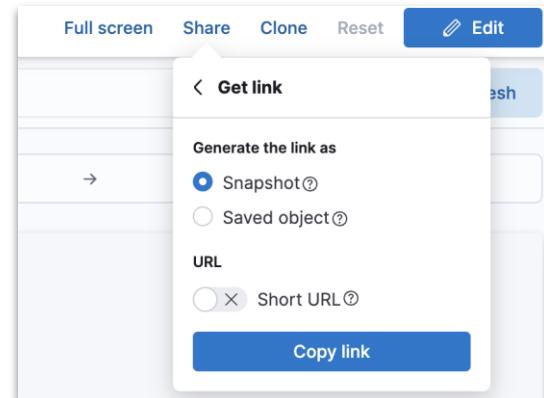
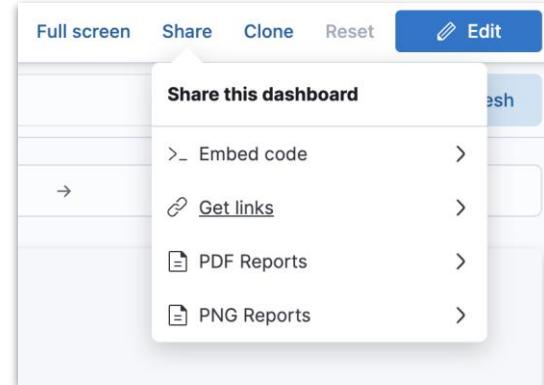
xpackCustomBranding.faviconSVG  
https://elastic-ml-workshop.s3.eu-central-1.amazonaws.com/icons.svg  
Reset to default

xpackCustomBranding.faviconPNG

**The Cool Company**

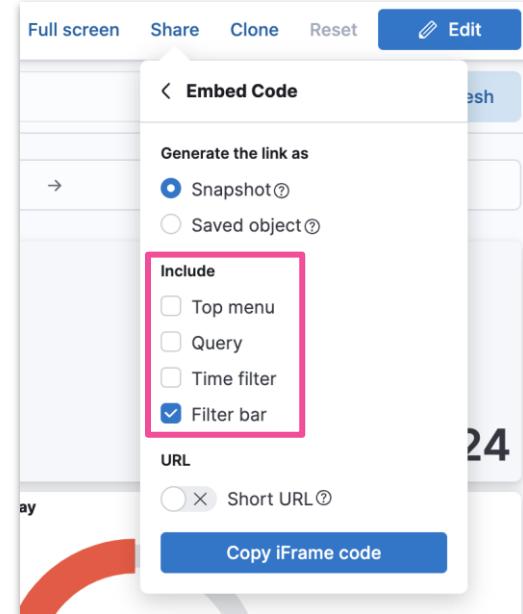
# Direct links

- Authentication required
  - Unless you setup anonymous auth
- Also works for
  - saved searches
  - visualizations (some)
- For a link to latest dashboard state
  - select either Saved Object
  - or Snapshot from a saved dashboard
- For a link to current dashboard state
  - select Snapshot from an unsaved dashboard



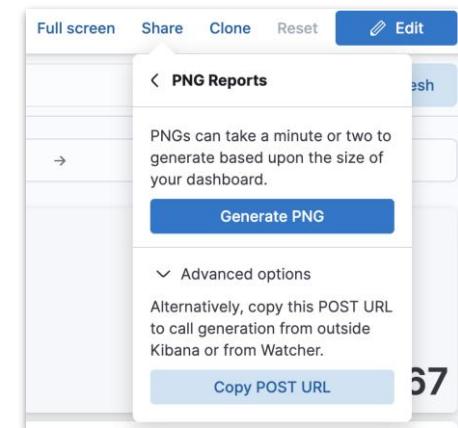
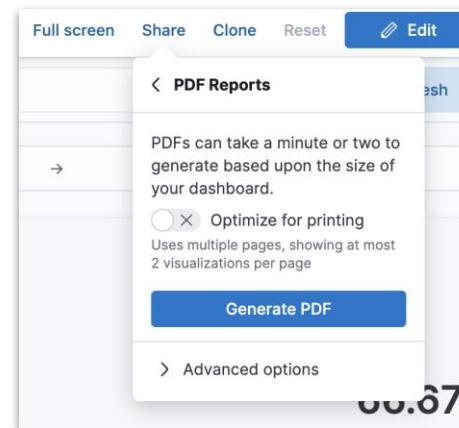
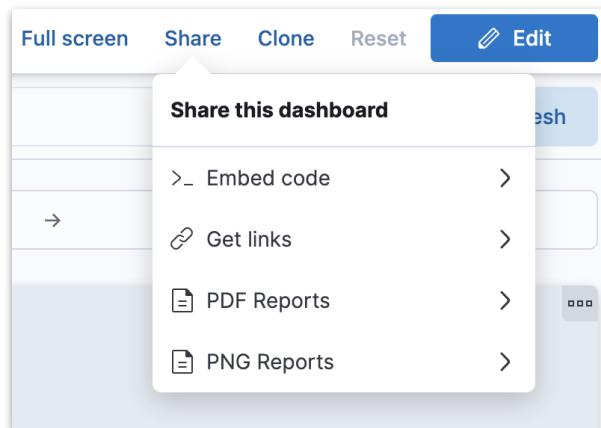
# Embed Code

- Embed dashboard as HTML code
  - Internal company website / web page
- For users with no Kibana access
  - Enable Kibana anonymous auth
    - `xpack.security.sameSiteCookies: None`



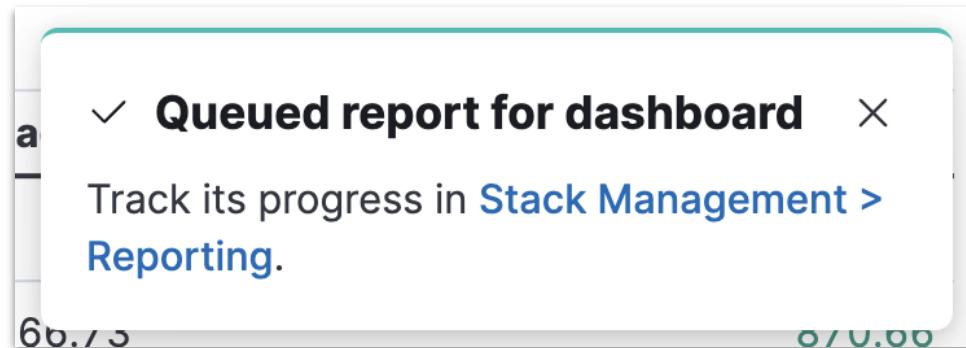
# Kibana reports

- A dashboard may also be shared as a report
  - PDF for printing
  - PNG for presentations



# Report generation

- Once created, the report will be available in **Stack Management**
- The **POST URL** can also be used to create scheduled reporting

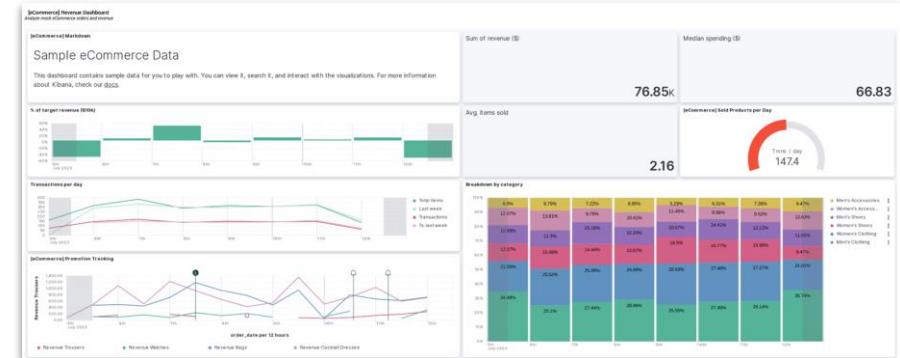


# Reports can be downloaded and deleted

## Reports

Get reports generated in Kibana applications.

<input type="checkbox"/> T...	Title	Status	Created at	Content	Actions
<input type="checkbox"/>	[eCommerce] Revenue Dashboard	 Done	2023-07-12 @ 11:53 AM	PDF 	



# Summary: Sharing a Dashboard

Module 5 Lesson 1

# Summary

- Live dashboards can be shared as embedded frames or links
  - both can be shared as snapshots or saved objects
- Viewing a live dashboard still requires a login
- Dashboards may also be shared statically as PDFs or PNGs

# Quiz

1. **True or False:** Reports can only be generated from the dashboard
2. **True or False:** A direct link will only show the data that was available when the link was created
3. When would you use a PDF report?



# Sharing a Dashboard

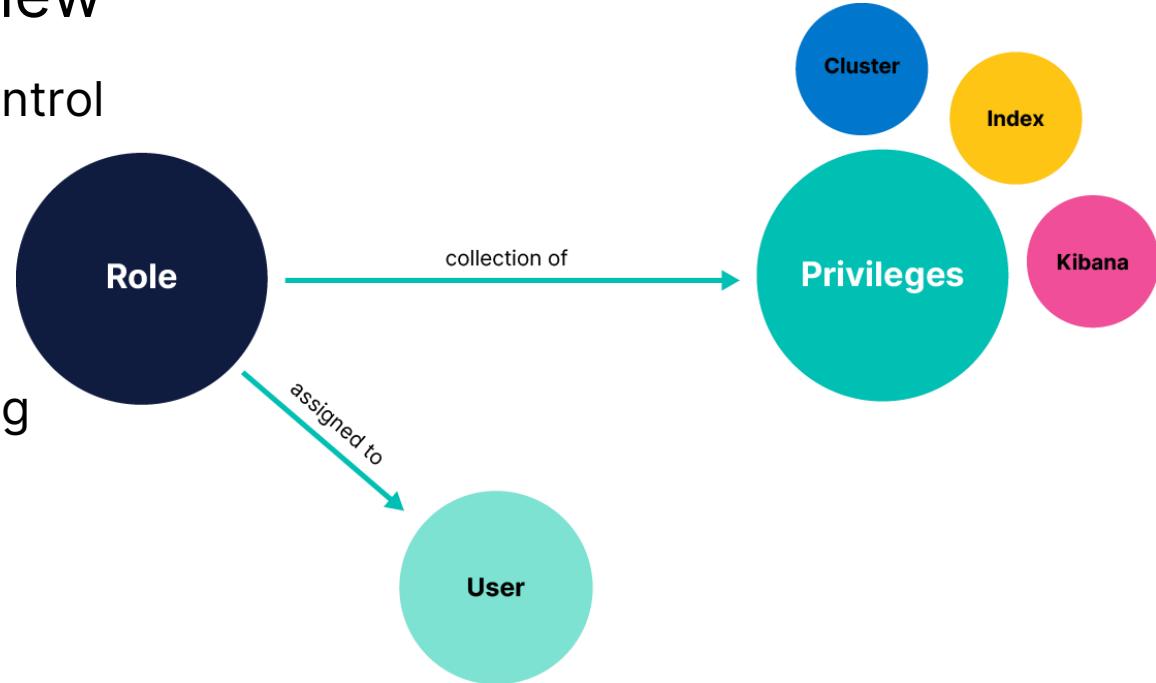
Lab 5.1 - Links and PDFs for sharing

# Sharing with users

Module 5 Lesson 2

# Kibana RBAC Overview

- Role-based access control
- Kibana features
  - analytics
  - management
  - solutions
- Granted through config
  - space + role



# Elasticsearch role config

## Elasticsearch hide

### Cluster privileges

Manage the actions this role can perform against your cluster. [Learn more](#)

Add an action...

Elasticsearch Cluster admin operations

### Run As privileges

Allow requests to be submitted on behalf of other users. [Learn more](#)

Add a user...

Submit requests on behalf of another user

### Index privileges

Control access to the data in your cluster. [Learn more](#)

Elasticsearch data privileges

#### Indices

Add an index pattern...

#### Privileges

Add an action...

Grant access to specific fields

Grant / Deny field level access

Grant read privileges to specific documents

Grant Doc level access

[+ Add index privilege](#)

Add another set of index privileges



# Kibana Role config

## Stack Management > Roles

This role does not grant access to Kibana

Add Kibana privilege

## Stack Management > Spaces

Feature visibility

Analytics

Discover

Dashboard

Canvas

Maps

Machine Learning

Graph

Visualize Library

4/7 features visible

For a user to be able to use a feature, it should be enabled in both **Spaces** and **Role** configs

Select space

Spaces

demo

Privileges for all features

All	Read	Customize
All	Read	Customize

Assign the privilege level you wish to grant to all present and future features across this space.

Customize by feature

Increase privilege levels on a per feature basis. Some features might be hidden by the space or affected by a global space privilege.

Customize feature privileges

Bulk actions ▾

Analytics			
	All	Read	None
Discover	All	Read	None
Dashboard	All	Read	None
Canvas	All	Read	None
Maps	All	Read	None
Machine Learning	All	Read	None
Graph	All	Read	None
Visualize Library	All	Read	None

4 / 7 features granted

Observability

Analytics

Security

Management

0 / 5 features granted

0 / 2 features granted

0 / 12 features granted

# Share a Dashboard through a space

- Create a space
- Share Dashboard
  - copy to new space
- Create a role with read privileges
  - in the new space
  - for relevant indices
- Assign user to the new role

# Create a space

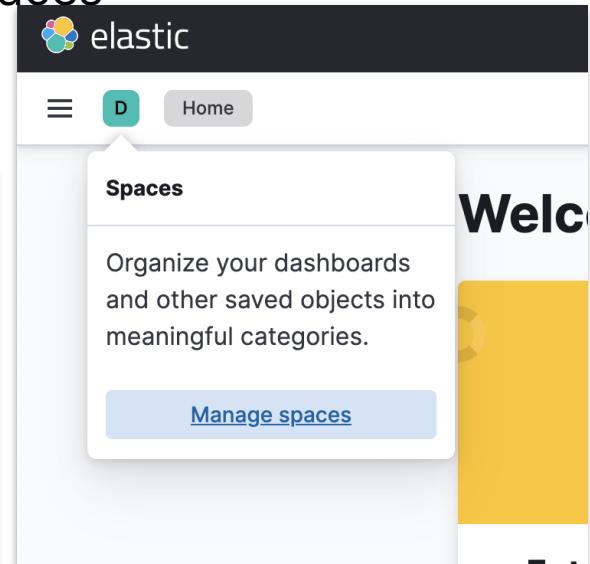
- Go to the Spaces Manager from
  - Spaces menu -> Manage spaces
  - Main menu -> Stack Management -> Spaces
- Enable / Disable features
  - Dashboard is under Analytics

**Features**

**Set feature visibility**

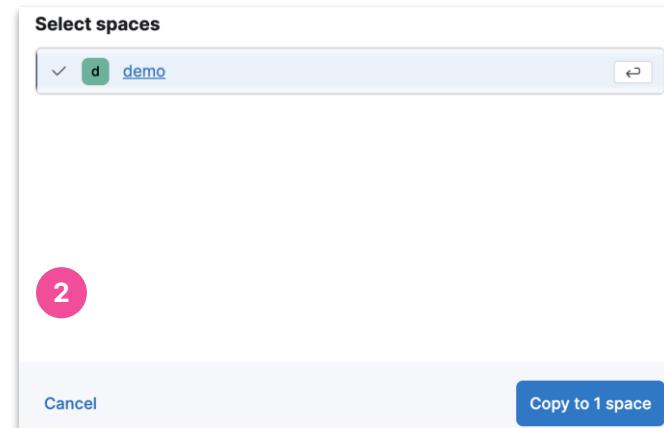
Hidden features are removed from the user interface, but not disabled. To secure access to features, [manage security roles](#).

Feature visibility	Show all	Hide all
<input checked="" type="checkbox"/>  Analytics	7/7 features visible >	
<input type="checkbox"/>  Enterprise Search		
<input type="checkbox"/>  Observability	0/5 features visible >	
<input type="checkbox"/>  Security	0/2 features visible >	
<input type="checkbox"/>  Management	0/12 features visible >	



# Copy dashboard to space

- Stack Management -> Saved Objects
  - Actions -> Copy to spaces
  - Select space
  - Copy to space
- Related objects will also be copied
  - Data views
  - Saved searches
  - Visualizations



The screenshot shows a table of saved objects. At the top left is a search bar with a magnifying glass icon and the placeholder 'Search...'. To its right is a pink circle containing the number '1'. On the far right of the table are filter buttons for 'Type', 'Tags', 'Delete', and 'Export'. The table has columns for 'Type', 'Title', 'Tags', 'Spaces', 'Last updated', and 'Actions'. There are three rows of data. The last row, which is highlighted with a pink rectangle around the 'Actions' column, has a 'Copy to spaces' button in the 'Actions' column. The 'Spaces' column for this row contains a green button with the letter 'D'.

Type	Title	Tags	Spaces	Last updated	Actions
<input type="checkbox"/>	[Logs] Web Traffic		—	22 h	<input type="button" value="Inspect"/> <input type="button" value="Relationships"/>
<input type="checkbox"/>	[eCommerce] Revenue Dashboard		—	yester	<input type="button" value="Relationships"/>
<input type="checkbox"/>	kibana_sample_data_ecommerce		D	2 da	<input type="button" value="Copy to spaces"/> <input type="button" value="Relationships"/>

# Create role with privileges

**Create role**

Set privileges on your Elasticsearch data and control access to your Kibana spaces.

Role name: demo

**Elasticsearch** hide

**Cluster privileges**  
Manage the actions this role can perform against your cluster. [Learn more](#)

**Run As privileges**  
Allow requests to be submitted on behalf of other users. [Learn more](#)

**Index privileges** 2  
Control access to the data in your cluster. [Learn more](#)

Indices: kibana\_sample\_data\_ecommerce x

Privileges: read x

Grant access to specific fields  
 Grant read privileges to specific documents

[+ Add index privilege](#)

**Kibana** hide

This role does not grant access to Kibana

[+ Add Kibana privilege](#)

**Kibana privileges** 4

**Spaces**  
demo x

Select one or more Kibana spaces to which you wish to assign privileges.

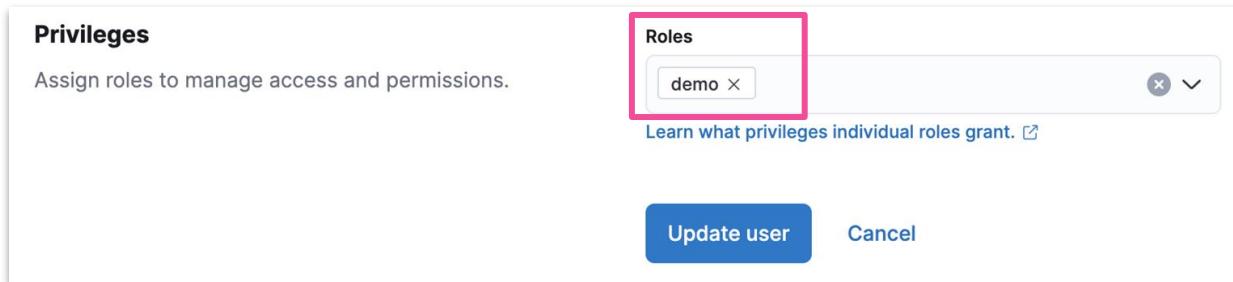
**Privileges for all features**

All Read Customize

Assign the privilege level you wish to grant to all present and future features across this space.

# Assign a Role to a User

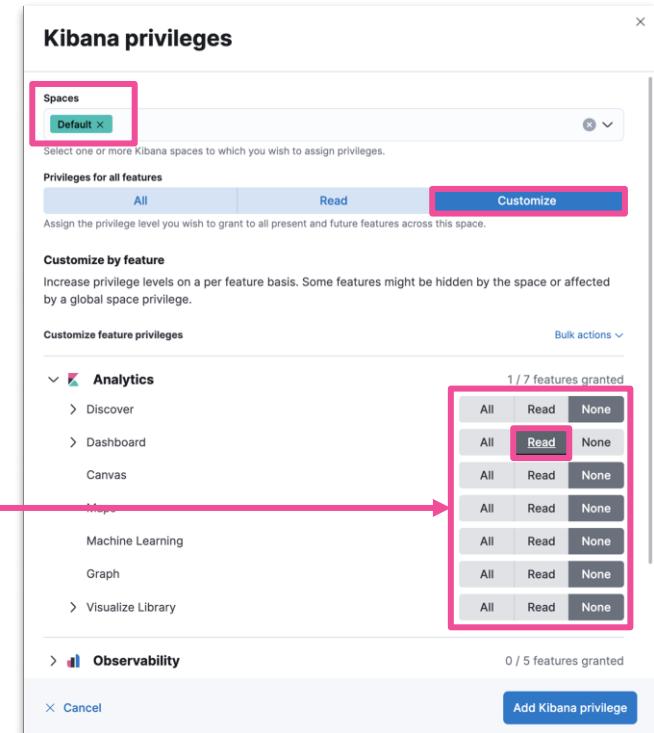
- Stack Management -> Users
  - Assign the Role to a User
- The new user will be able to access the new space with the shared dashboard



# Alternatively

- Provide limited access in **existing** space
  - Create a role with limited privileges
    - in existing space
    - for relevant indices
  - Assign user to the new role

You can also individually customize privileges by features



# Anonymous authentication

- Give users access to Kibana without requiring credentials
  - making it easier to share specific dashboards for example
- Beware! All access to Kibana will be anonymous
  - make sure you restrict what the anonymous users can access
- See: [elastic.co/guide/en/kibana/current/kibana-authentication.html#anonymous-authentication](https://elastic.co/guide/en/kibana/current/kibana-authentication.html#anonymous-authentication)

# Summary: Sharing with users

Module 5 Lesson 2

# Summary

- **Roles** provide authorization
- **Users** provide authentication
- When sharing a dashboard with a wide audience, consider anonymous authentication, with limited privileges

# Quiz

1. Which provides authorization to specific actions – **Users** or **Roles**?
2. When using an anonymous login to Kibana, what is an issue to be aware of?
3. How can spaces be used to provide limited access to Kibana features?

# Sharing with users

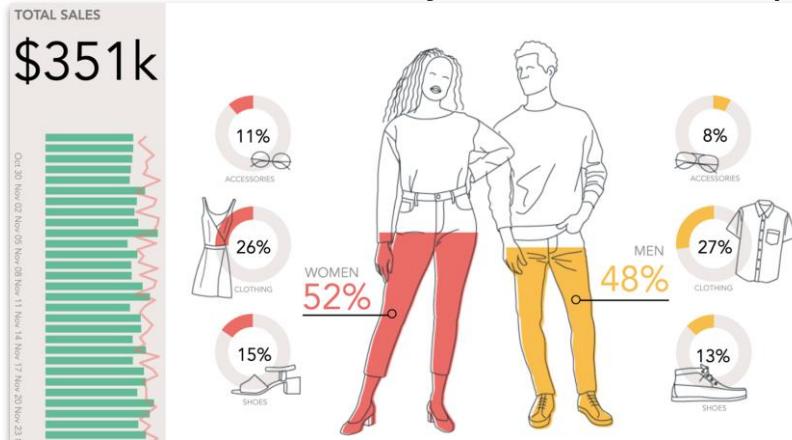
Lab 5.2 - Create a role and user to view  
Dashboards

# Canvas

Module 5 Lesson 3

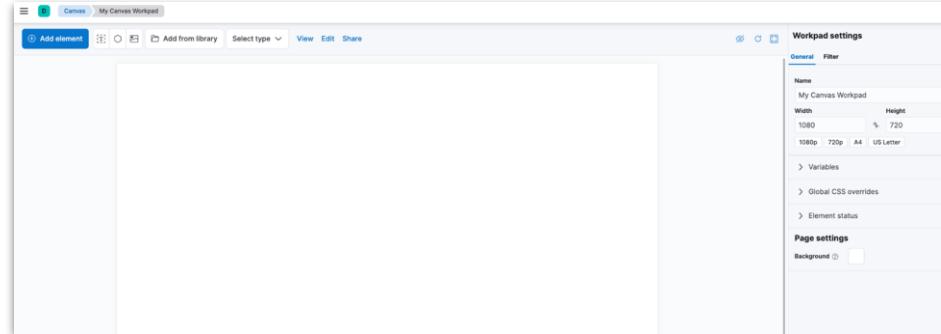
# Canvas

- Pull live data
- Present using rich infographics
  - colors, images, text
  - charts, graphs, progress monitors
- Focus the data you want to display with filters



# Getting started with Canvas

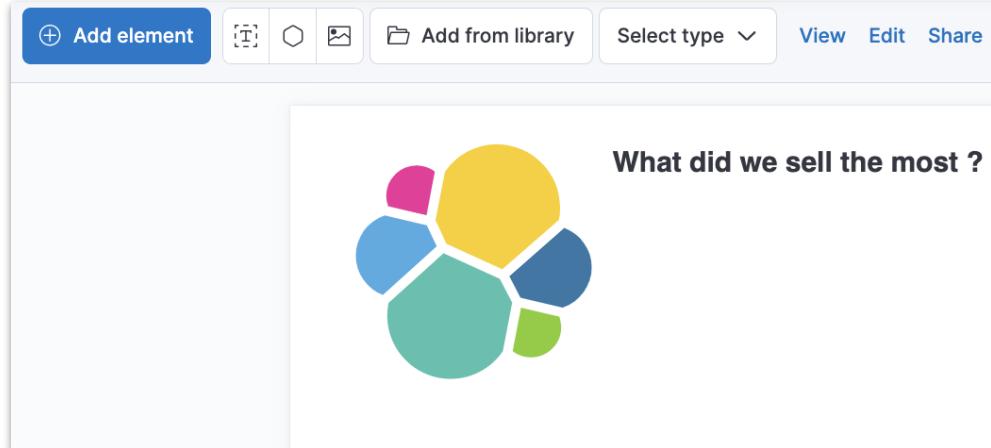
- To get started with Canvas:
  - click **Canvas** from the Kibana main menu
  - **Create workpad**, optionally using a **Template**
  - click **Add element** in the top left



- Elements can be placed anywhere and resized to achieve the desired layout

# Static elements

- Static content, like text and images, are simple to add
  - text uses Markdown



# Visualization library

- Any visualization that is saved to the library may be added as a **Kibana element**

### Add from library

Search... Sort ▾ Types 4 ▾

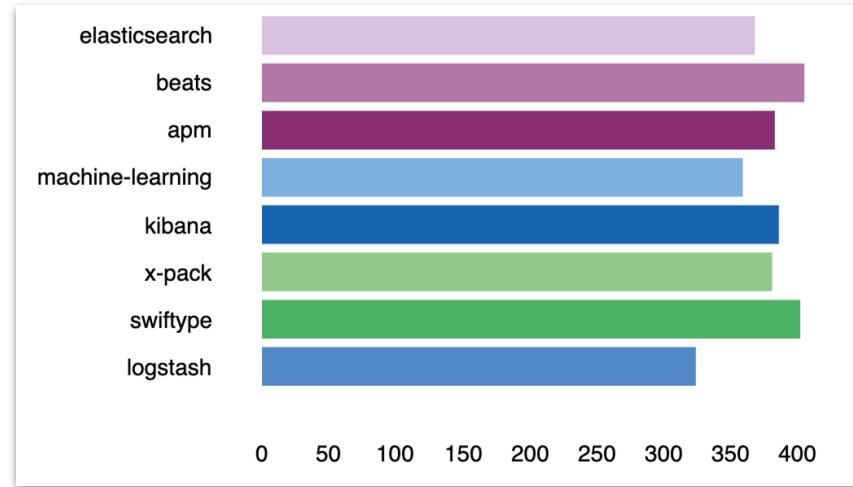
- ≈ [eCommerce] Controls
- ≡ [eCommerce] Markdown
- ⌚ [eCommerce] Orders
- ⌚ [eCommerce] Orders by Country
- 📊 [eCommerce] Promotion Tracking
- 📊 [eCommerce] Promotion Trackings
- ⚡ [eCommerce] Sales Count Map
- 📊 [eCommerce] Sold Products per Day
- ⌚ [Logs] Bytes distribution
- ⌚ [Logs] Goals

Rows per page: 10 < 1 2 3 >

- Visualization
- Saved search
- Lens Visualization
- Map

# Canvas elements

- Canvas supports many familiar elements



- And also some that are unique to Canvas

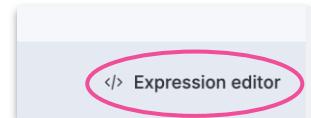
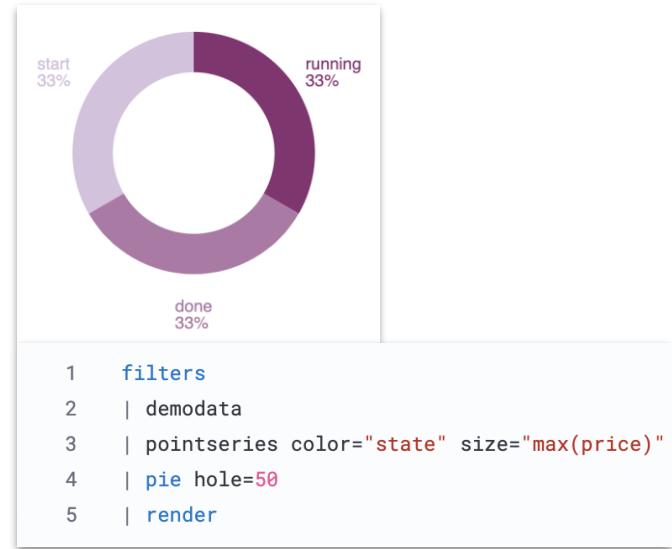


# Data Sources

- Every Canvas element has a **data source**
- Several types of data source are supported:
  - **Elasticsearch SQL**: data in Elasticsearch, accessed using the Elasticsearch SQL syntax
  - **Elasticsearch documents**: data in Elasticsearch, using the Lucene syntax
  - **Demo data**: small sample dataset that is used when you first create a new element
  - **Timelion**: data in Elasticsearch, using the Timelion syntax

# Canvas Expression

- Defines how to
  - retrieve data
  - manipulate
  - visualize in element
- Executes functions
  - produces outputs
  - passed on to next function



# Functions

```
1 filters
2 | demodata
3 | table
4 | render
```

```
1 filters
2 | demodata
3 | pointseries color="state" size="max(price)"
4 | pie hole=50
5 | render
```

- 1 Provide the values of any time filters or dropdown filters in the workpad
- 2 Canvas sample data
- 3 Create table visualization
- 4 Render the element and set options

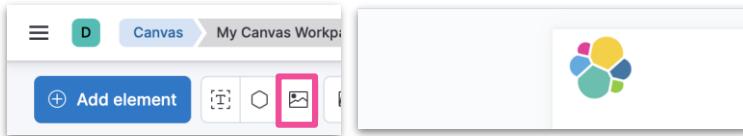
@timestamp	time	cost	#	username	t	price	#	age	#
2019-01-01T04:16:51-05:00	2019-01-01T04:16:51-05:00	32.15	aevans2e	53	63				
2019-01-01T09:05:51-05:00	2019-01-01T09:05:51-05:00	20.52	aking2c	33	68				

- 1 Provide the values of any time filters or dropdown filters in the workpad
- 2 Canvas sample data
- 3 Aggregate data
- 4 Configure a pie chart element
- 5 Render the element and set options

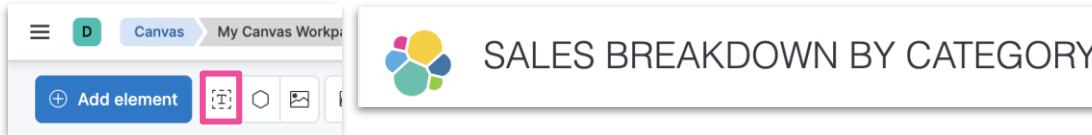


# Canvas example

1



2



3

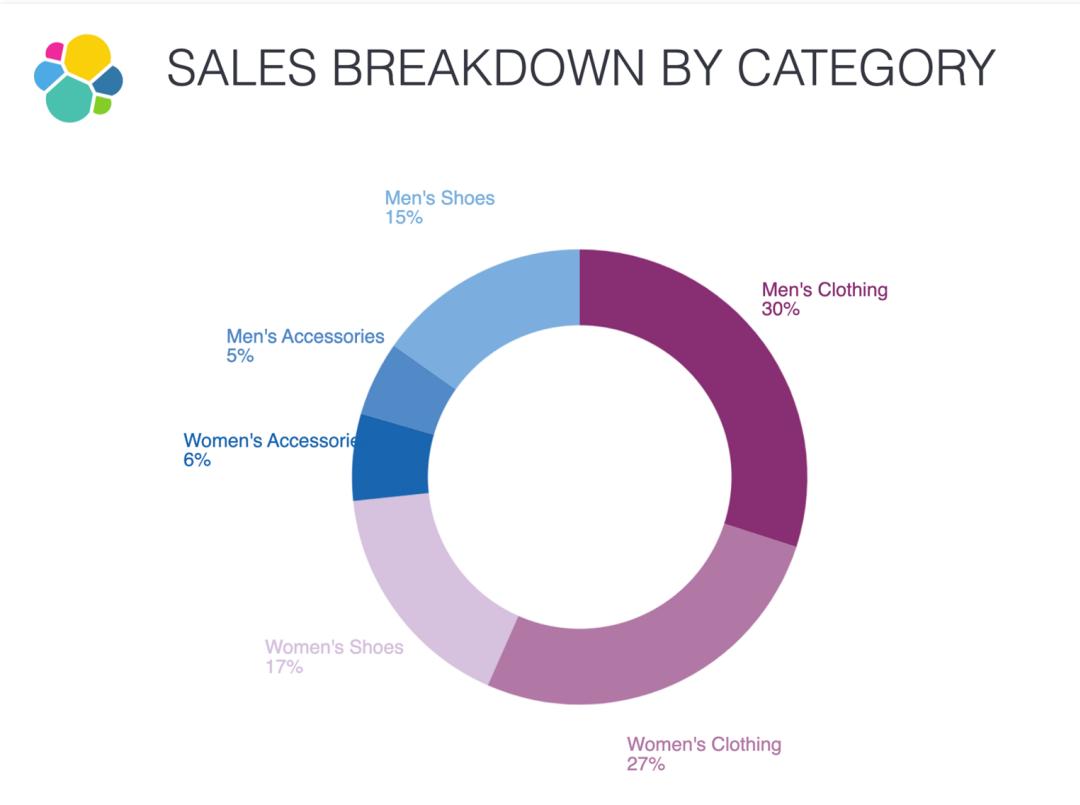
A screenshot of the Kibana Canvas interface showing the configuration of a pie chart element. On the left is a sidebar with various chart types: Area, Bubble, Coordinate plot, Data table, Heatmap, Horizontal bar, Line, and Metric (highlighted with a pink box). The main panel shows the 'Selected element' configuration with tabs for 'Display', 'Data' (selected), and 'Filters'. Under 'Data', there's an 'Elasticsearch SQL' section with a 'Query' field containing the following code:

```
SELECT category.keyword,
       taxful_total_price FROM
      "kibana_sample_data_ecommerce"
```

The entire 'Data' configuration section is highlighted with a pink box.

```
1 kibana
2 | selectFilter
3 | essql
4 | query="SELECT category.keyword, taxful_total_price FROM \"kibana_sample_data_ecommerce\""
5 | pointseries color="category.keyword" size="sum(taxful_total_price)"
6 | pie hole=50
7 | render
```

# Canvas example



# PDFs with infographics

- Export a Workpad to PDF to generate a report with rich infographics



# Summary: Canvas

Module 5 Lesson 3

# Summary

- **Canvas** provides a platform for creating presentations with live data
- Canvas **elements** are used to build the various views of the data
- Some elements display static content, like text and images
- Any **visualization** saved to the library may be added to a workpad

# Quiz

1. **True or False:** Lens visualizations may be used in Canvas.
2. Name data sources that can be used in data-driven elements.
3. What is the first step when creating a Canvas presentation?

# Canvas

Lab 5.3 - Build a simple Canvas presentation

# Additional Links

- Elasticsearch SQL:  
<https://www.elastic.co/guide/en/elasticsearch/reference/current/sql-spec.html>
- Timelion:  
<https://www.elastic.co/guide/en/kibana/current/timelion.html>
- Canvas tutorial: <https://www.elastic.co/guide/en/kibana/current/canvas-tutorial.html>

# Data Analysis with Kibana: Agenda

- Getting Started
- Search your Data
- Visualize your Data
- Additional Visualizations
- Present your Data
- **Analyze your Data with Machine Learning**
- Advanced Kibana
- Alerting

# Analyze your data with machine learning

Module 6

# Lessons

- Introduction to Elastic Machine Learning
- Analyzing anomaly detection results
- Data frame analytics
- AIOps Labs

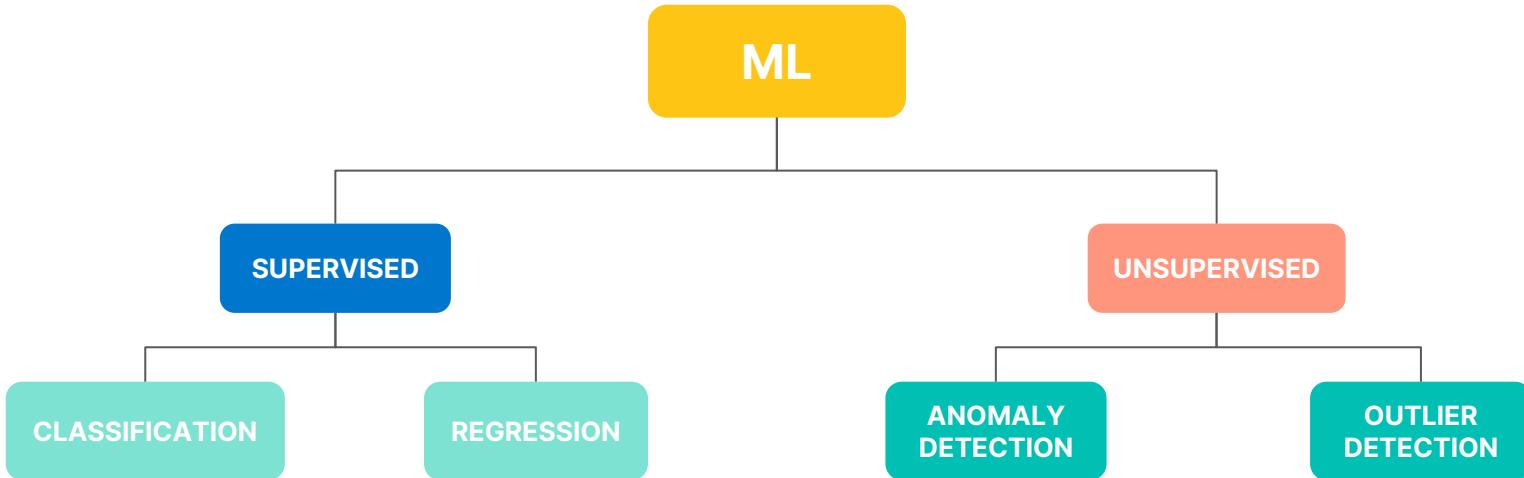
# Introduction to Elastic Machine Learning

Module 6 Lesson 1

# Machine learning in the Elastic Stack

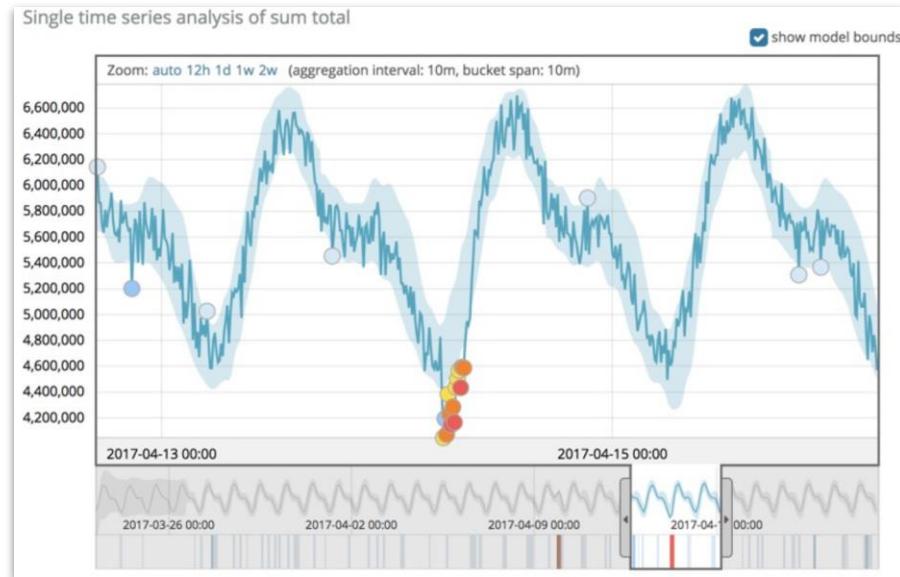
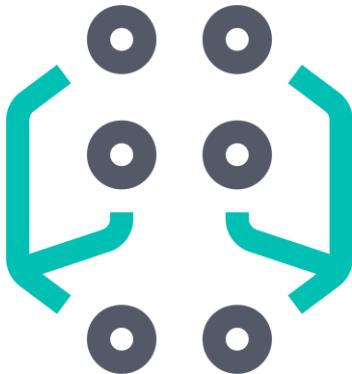
- The Elastic Stack supports several data analysis use cases using supervised and unsupervised machine learning (ML)
  - anomaly detection
  - forecasting
  - language identification
- The goal is to **operationalize** and **simplify** data science
- In this course, we will cover **anomaly detection** and **outlier detection** as examples

# Elastic Machine Learning



# Anomaly detection

- Identify patterns and unusual behavior in historical and streaming time series data



# Anomaly detection

Is the log rate significantly higher than usual?

Is the log rate significantly lower than usual?

Is the log rate fluctuating when expected?

Is there a significant spike in any of my system metrics?

Are there an unusually high number of authentication attempts?

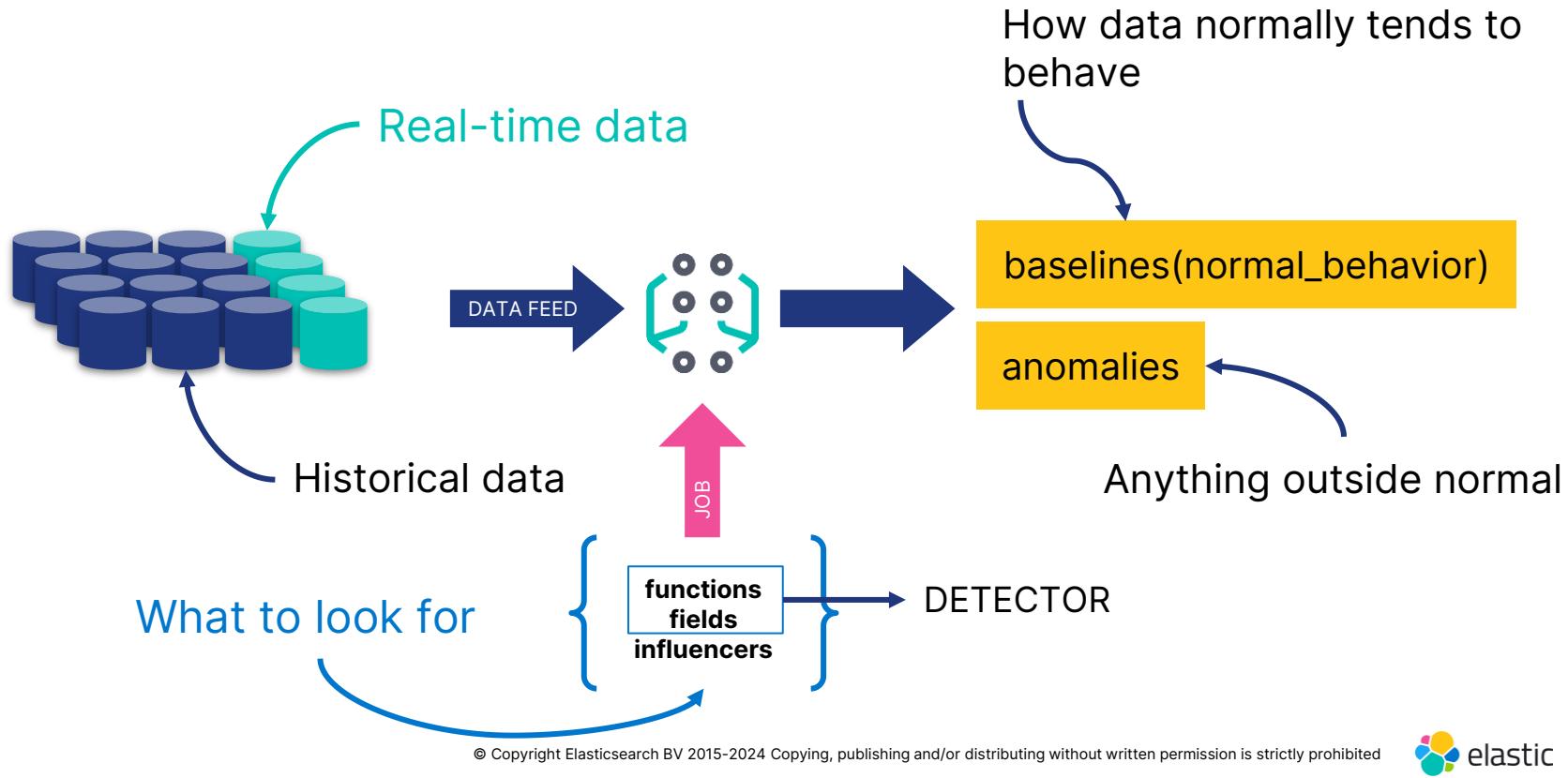
Are there any unusual user names in the authentication logs?

Are there any unusual processes using the network?

Are there any unusual destination port activity?

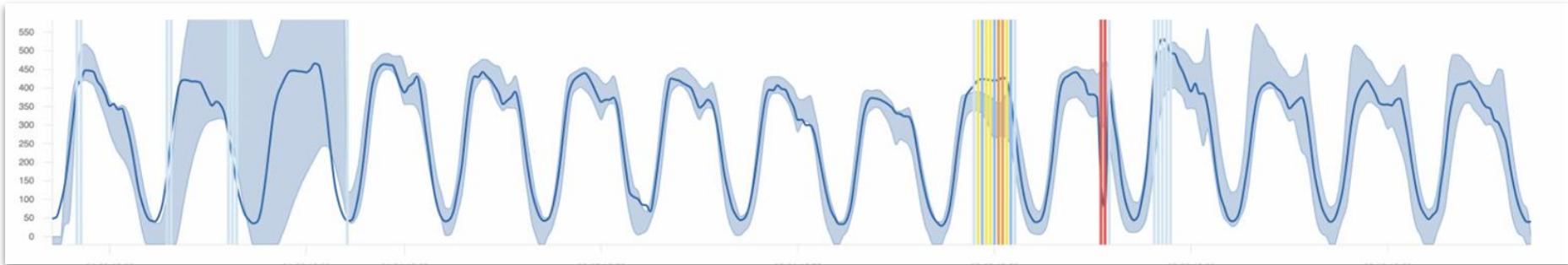


# Anomaly detection



# Let's create a job

- What kinds of patterns can we find in time series data?
- The next slides cover configuring a single metric job



# 1. Choose a job type from the available

wizard

Use a wizard

## Single metric

Detect anomalies in a single time series.

## Multi-metric

Detect anomalies with one or more metrics and optionally split the analysis.

## Population

Detect unusual activity in a population. Recommended for high cardinality data.

## Advanced

Use the full range of options to create a job for more advanced use cases.

## Categorization

Group log messages into categories and detect anomalies within them.

## Rare

Detect rare values in time series data.

## Geo

Detect anomalies in the geographic location of the data.

## Learn more about your data

If you're not sure what type of job to create, first explore the fields and metrics in your data.

## Data Visualizer

Learn more about the characteristics of your data and identify the fields for analysis with machine learning.

## 2. Define the time range

**Create job: Single metric**

Using data view Kibana Sample Data eCommerce (kibana\_sample\_data\_ecommerce)

1 Time range 2 Choose fields 3 Job details 4 Validation 5 Summary

**Time range**

Jul 13, 2023 @ 02:04:19.000 → Jul 27, 2023 @ 11:39:48.918 Use full data

Next >

# 3. Choose field and metric (detector)

## Create job: Single metric

Using data view Kibana Sample Data eCommerce (kibana\_sample\_data\_ecommerce)

1 Time range      2 Choose fields      3 Job details      4 Validation      5 Summary

### Choose fields

Sum(taxful\_total\_price) |

sku  
Distinct count(sku)

# taxful\_total\_price  
Mean(taxful\_total\_price)  
High mean(taxful\_total\_price)  
Low mean(taxful\_total\_price)

Sum(taxful\_total\_price)

The chart displays the sum of taxful total price over time. A prominent vertical spike occurs around July 17, reaching a value of approximately 1000. The signal then settles into a lower, more stable level with smaller fluctuations.

# 4. Define bucket span

**Bucket span**  
The interval for time series analysis, typically 15m–1h.

1h

[Convert to multi-metric job](#)

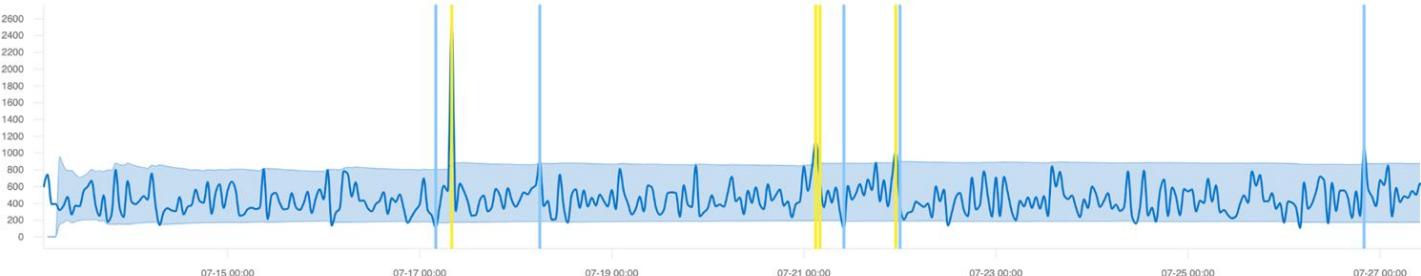
Sparse data  
Ignore empty buckets from being considered anomalous. Available for count and sum analysis.

< Previous

The bucket span is one hour

# 5. Create job and view results

New job from data view Kibana Sample Data eCommerce



<b>Job ID</b> demo	<b>Bucket span</b> 1h	<b>Enable model plot</b> True	<b>Start</b> Jul 13, 2023 @ 02:04:19.000
<b>Job description</b> <i>No description provided</i>	<b>Influencers</b> <i>No influencers selected</i>	<b>Use dedicated index</b> False	<b>End</b> Jul 27, 2023 @ 11:39:48.918
<b>Groups</b> <i>No groups selected</i>		<b>Model memory limit</b> 11MB	

Start immediately  
If unselected, job can be started later from the jobs list.

[View results](#) [Reset job](#) [Start job running in real time](#) [Create alert rule](#)

# Unusually high revenue



# Calendars and scheduled events

## Create new calendar

### Calendar ID

demo\_calendar

Use lowercase alphanumeric (a-z and 0-9), hyphens or underscores;  
must start and end with an alphanumeric character

### Description

Demo calendar functionality

Apply calendar to all jobs

### Jobs

demo\_low\_request\_rate

## Settings

### Anomaly Detection

#### Calendars

Calendars contain a list of scheduled events for which you do not want to generate anomalies, such as planned system outages or public holidays.

You have 0 calendars

Manage

Create

### Groups

kibana\_sample\_web\_logs

### Events

Search...

+ New event

Import events

Description ↑	Start	End	
Web Server Scheduled Maintenance	2022-10-24 00:00:00	2022-10-28 00:00:00	Delete

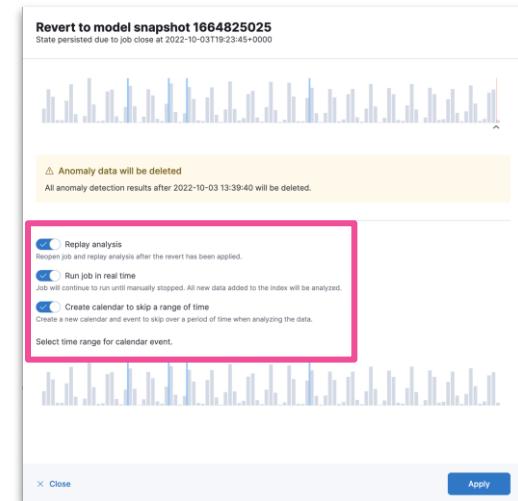
Rows per page: 5

< 1 >

# Restore model snapshots

- Snapshot saved frequently to an index
- Revert to a snapshot in case of
  - System failure
  - undesirable model change due to one off events

realtime1		1,409	ok	opened	started	2022-10-03 14:39:58	Actions				
Job settings	Job config	Datafeed	Counts	JSON	Job messages	Datafeed preview	Forecasts	Annotations	Model snapshots		
ID	Description				Date created ↑				Latest timestamp	Retain	Actions
1664825025	State persisted due to job close at 2022-10-03T19:23:45+0000				2022-10-03 15:23:45				2022-10-03 13:39:40	No	
1664825052	Periodic background persist at 2022-10-03T19:24:12+0000				2022-10-03 15:24:12				2022-10-03 14:39:58	No	



# Forecasting

- Given a model, predict future behavior



# Summary: Introduction to Elastic Machine Learning

Module 6 Lesson 1

# Summary

- Elastic enables you to analyse your data using **unsupervised** and **supervised** machine learning techniques
- Elastic **anomaly detection** uses unsupervised machine learning to find unusual patterns in your time series data
- Anomaly detection uses a **job** to create a **model** of how your data is expected to behave over time
- Configure a **calendar** to exclude future time frames from analysis, or **revert** to an earlier **model snapshot** after the fact
- A model can be used to **forecast** future behavior

# Quiz

- 1. True or False:** The best way to find anomalies in time series data is to check all your dashboards every hour and closely look for something that is out of the ordinary.
2. What two mechanisms can be used to exclude events from anomaly detection analysis?
3. When would you use each method?

# Introduction to Elastic Machine Learning

Lab 6.1 - Single- and multi-metric jobs

# Analyzing anomaly detection results

Module 6 Lesson 2

# Actionable machine learning

- After you have created a model of your data, and detected anomalies, you may want to:
  - Analyze and enrich the results
  - Share your results within a Dashboard

# Tools for analysis

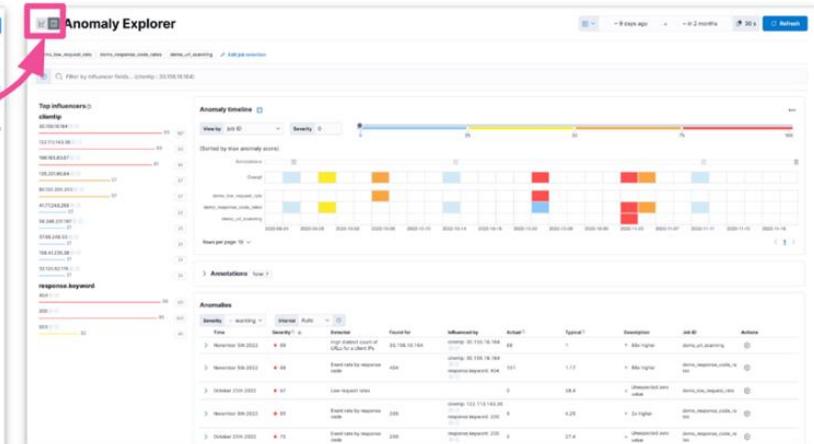
## Single Metric Viewer

- Display single time series
- Chart of Actual vs Expected (95%)
  - Blue line
  - Blue shade



## Anomaly Explorer

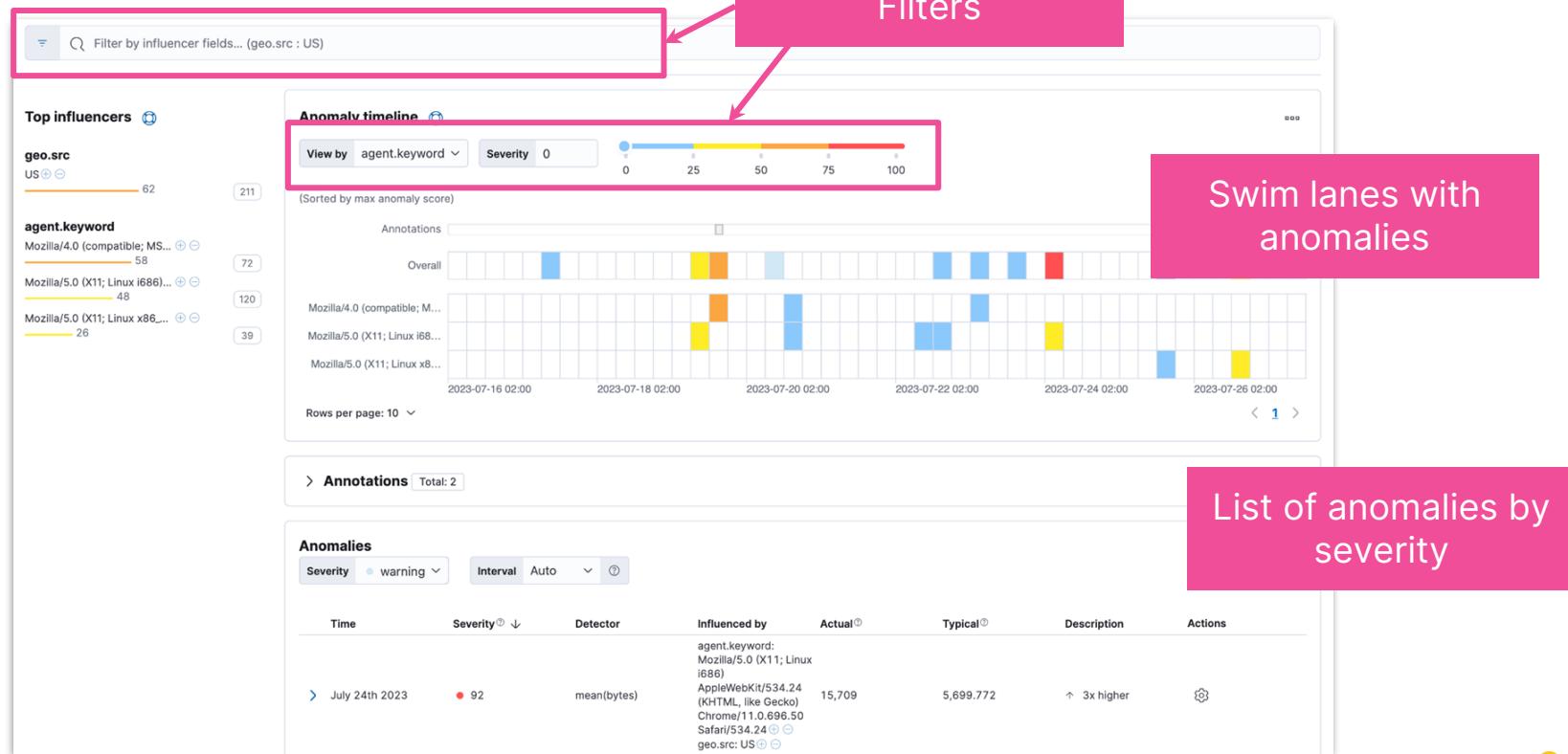
- Swimlanes for different job results
  - Overall score
  - Shared influencers



# Single metric viewer



# Anomaly explorer



# Add swimlanes to dashboards

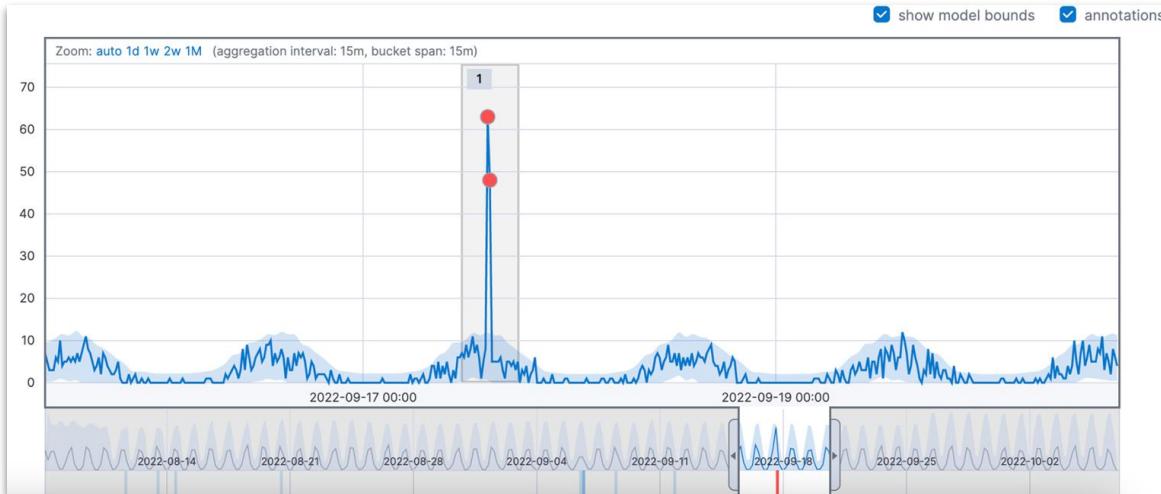
The screenshot shows the Elasticsearch Dashboard interface. At the top, there's a navigation bar with a menu icon, a 'Dashboard' button, and a 'Editing New Dashboard' title. Below the navigation is a search bar with a KQL syntax placeholder and a 'Create visualization' button.

A modal window titled 'Machine Learning' is open, showing two options: 'Anomaly swim lane' and 'Anomaly chart'. The 'Anomaly swim lane' option is selected and highlighted with a blue border. Below the modal, a large text area says 'Add your first visualization' and 'Create content that tells a story about your data.'

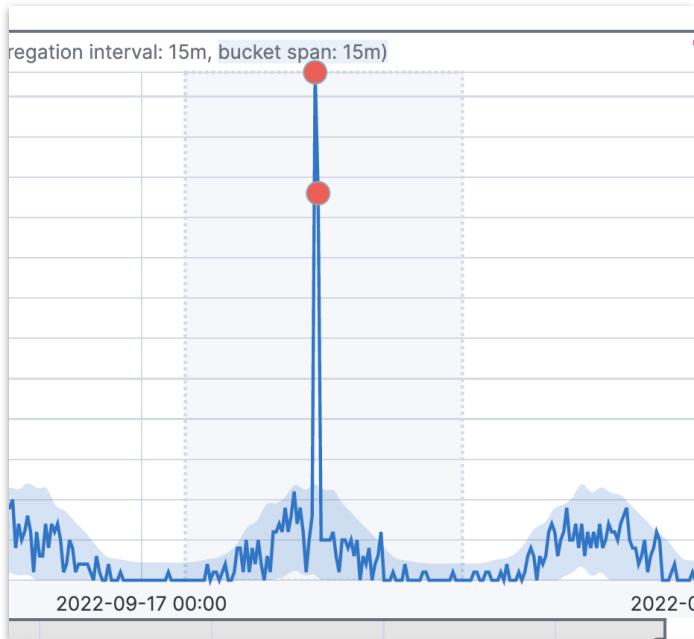
The main dashboard area displays a visualization titled 'Anomaly timeline'. It features a color scale from 0 to 100 for severity. The timeline shows several colored segments representing anomalies for different user agents over time. Annotations are visible above the timeline grid. On the right side of the visualization, there are buttons for 'Add to dashboard', 'Add to case', and navigation arrows. A legend at the bottom identifies the colors: Overall (light gray), Mozilla/4.0 (compatible; M... (blue), Mozilla/5.0 (X11; Linux i68... (yellow), Mozilla/5.0 (X11; Linux x8... (orange), and Mozilla/5.0 (Windows NT 10.0; Win... (red).

# Annotations

- When you run a machine learning job, its algorithm is trying to find anomalies — but it doesn't know what the data itself is about
- User annotations offer a way to augment the results with the knowledge you as a user have about the data



# Create annotations



Drag-select

Add annotation

Job ID	my_job
Start	September 17th 2022, 03:39:47
End	September 18th 2022, 02:48:04
Detector	count
Annotation text	System Reboot

Add your notes

Cancel Create

# Review your annotations



# Analyzing in other apps

## Create data view

Name

Enter an index pattern that matches one or more data sources. Use an asterisk (\*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.

Timestamp field

Select a timestamp field for use with the global time filter.

[Hide advanced settings](#)

Allow hidden and system indices

Custom data view ID

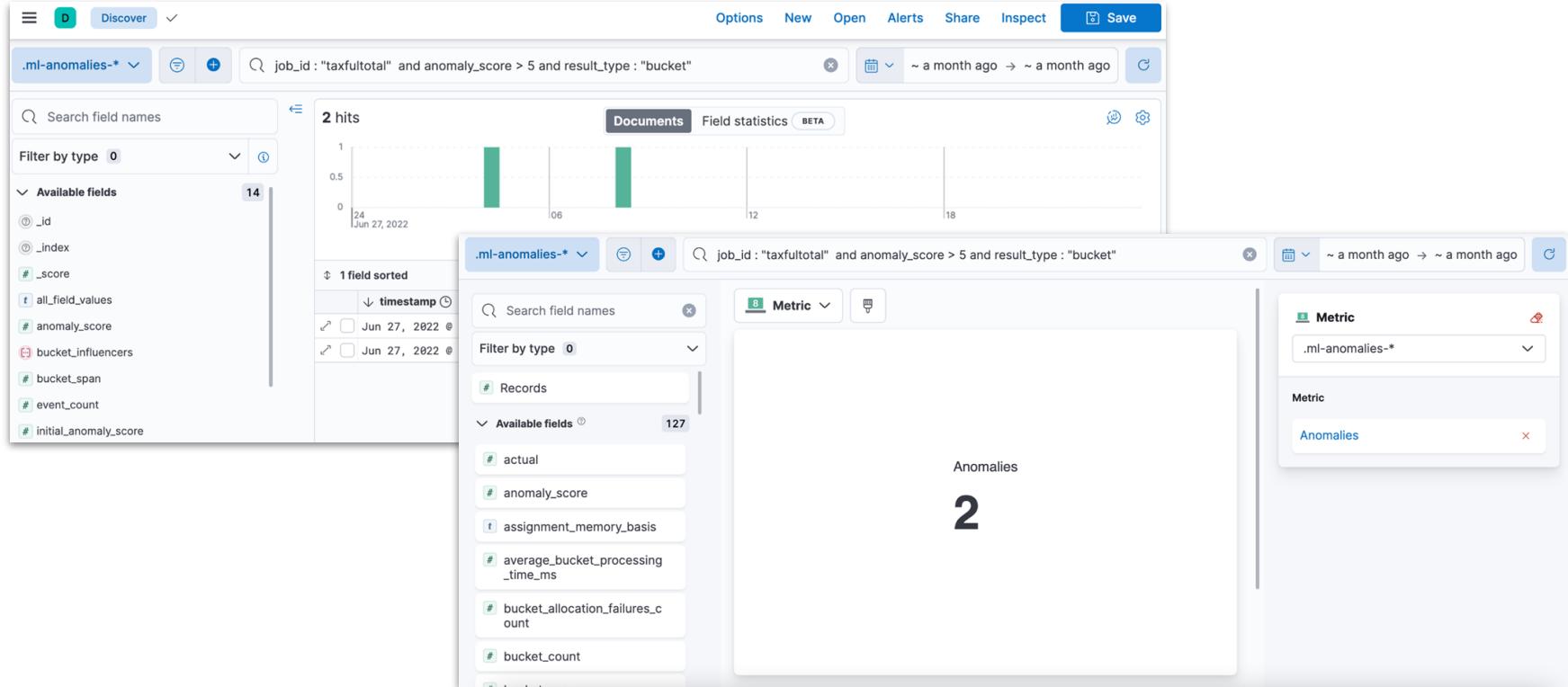
Kibana provides a unique identifier for each data view, or you can create your own.

✓ Your index pattern matches 7 sources.

.ml-anomalies-.write-demo_low_request_rate	Alias
.ml-anomalies-.write-demo_response_code_rates	Alias
.ml-anomalies-.write-demo_url_scanning	Alias
.ml-anomalies-demo_low_request_rate	Alias
.ml-anomalies-demo_response_code_rates	Alias
.ml-anomalies-demo_url_scanning	Alias
.ml-anomalies-shared	Index

Rows per page: 10 ▾

# Query and visualize the anomalies



# Summary: Analyzing anomaly detection results

Module 6 Lesson 2

# Summary

- Create annotations to highlight significant events
- You can add swimlanes and anomaly charts to dashboards to visualize anomalies
- Alternatively, you can visualize the data in the .ml-anomalies-\* indices

# Quiz

- 1. True or False:** Anomalies can be visualized using Kibana Lens like any other data.
- 2. True or False:** The result of machine learning jobs can only be viewed in Machine Learning.
- 3. True or False:** Annotations can be created from the Anomaly Explorer section.

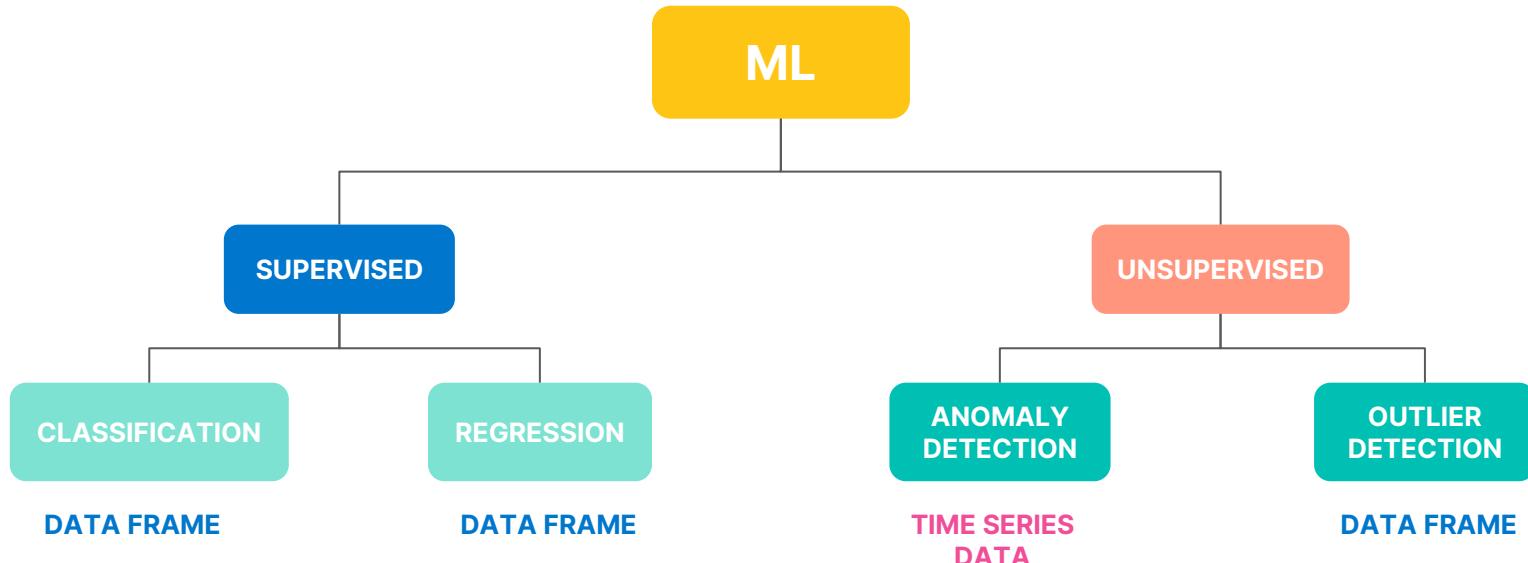
# Analyzing anomaly detection results

Lab 6.2 - Analyzing anomaly detection results

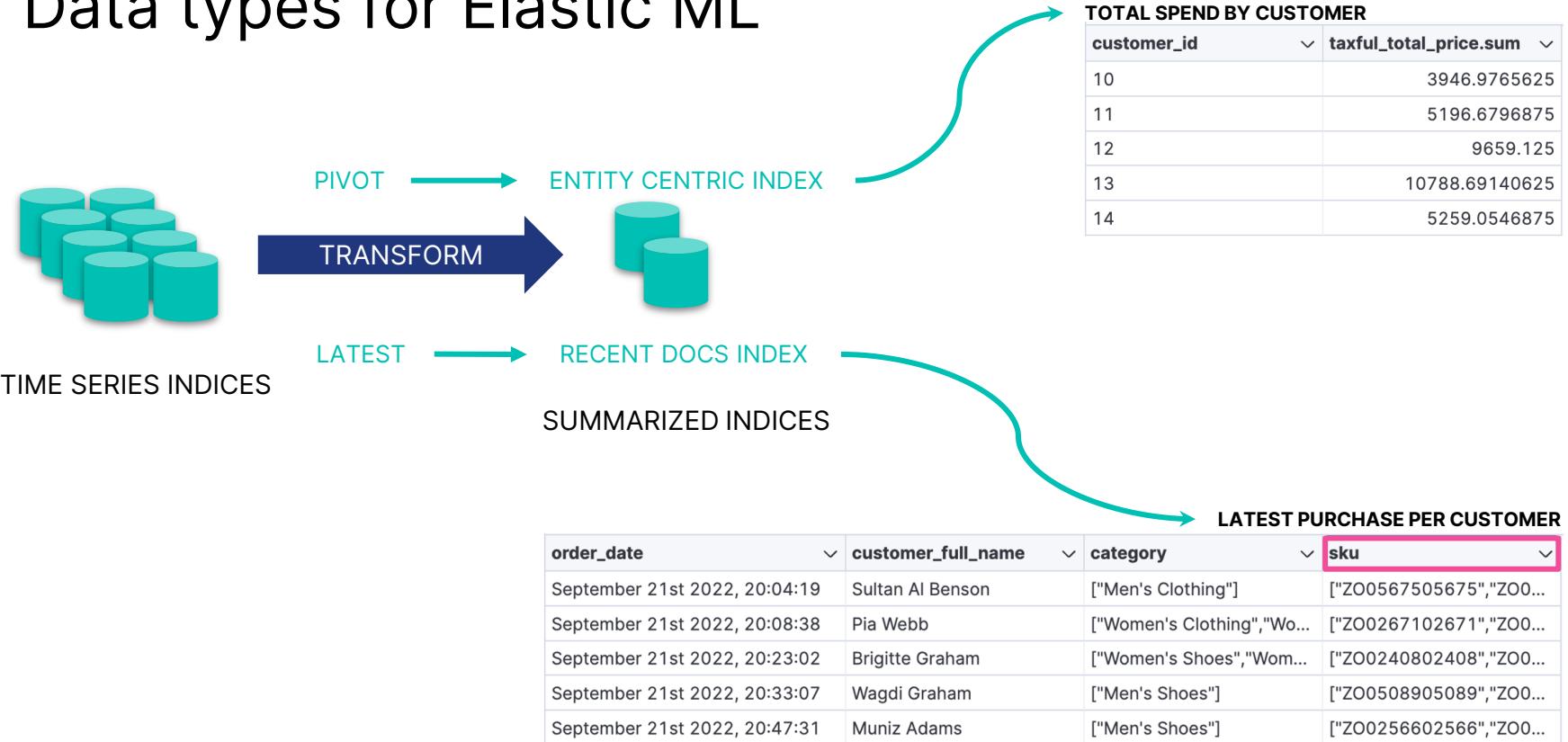
# Data frame analytics

Module 6 Lesson 3

# Data structures for Elastic ML



# Data types for Elastic ML



# Outlier detection example

- Based on the eCommerce orders, which customers are unusual?
  - customers who show fraudulent behavior
  - "VIP" customers who spend much more than others
- First, transform the data to a customer-centric index
- Next, detect outliers based on the relevant features

# Transform eCommerce orders

Transform configuration

Group by

customer\_id

Group by the id

Add a group by field ...

Aggregations

products.quantity.sum

taxful\_total\_price.sum

order\_date.value\_count

Add an aggregation ...

Fields you aggregate for each customer

Preview

Columns Sort fields

customer_id	order_date.value_count	products.quantity.sum	taxful_total_price.sum
10	59	118	3946.9765625
11	75	150	5196.6796875
12	135	270	9659.125
13	114	307	10788.69140625
14	72	143	5259.0546875

Rows per page: 5 < 1 2 3 4 5 ... 10 >

Check the preview of your transform

> Next

© Copyright Elasticsearch BV 2015-2024 Copying, publishing and/or distributing without written permission is strictly prohibited

elasticsearch

# Detect outliers

**Create job** Use the new customer index

Source data view: customer   Switch to json editor

**1 Configuration**



### Outlier detection

Identify unusual data points in the data set.

✓ Selected



### Regression

Predict numerical values in the data set.

Select



### Classification

Predict classes of data points in the data set.

Select

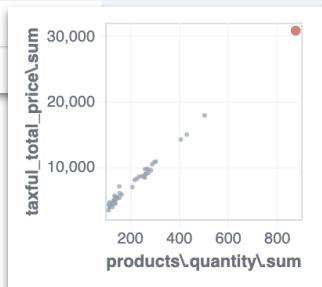
**Query**  Search for e.g. method : "GET" or status : "404"

# Detect outliers

- Select the fields you want analyze
- Review the results

Elyssa Barnes  
spends much more  
than typical  
customers

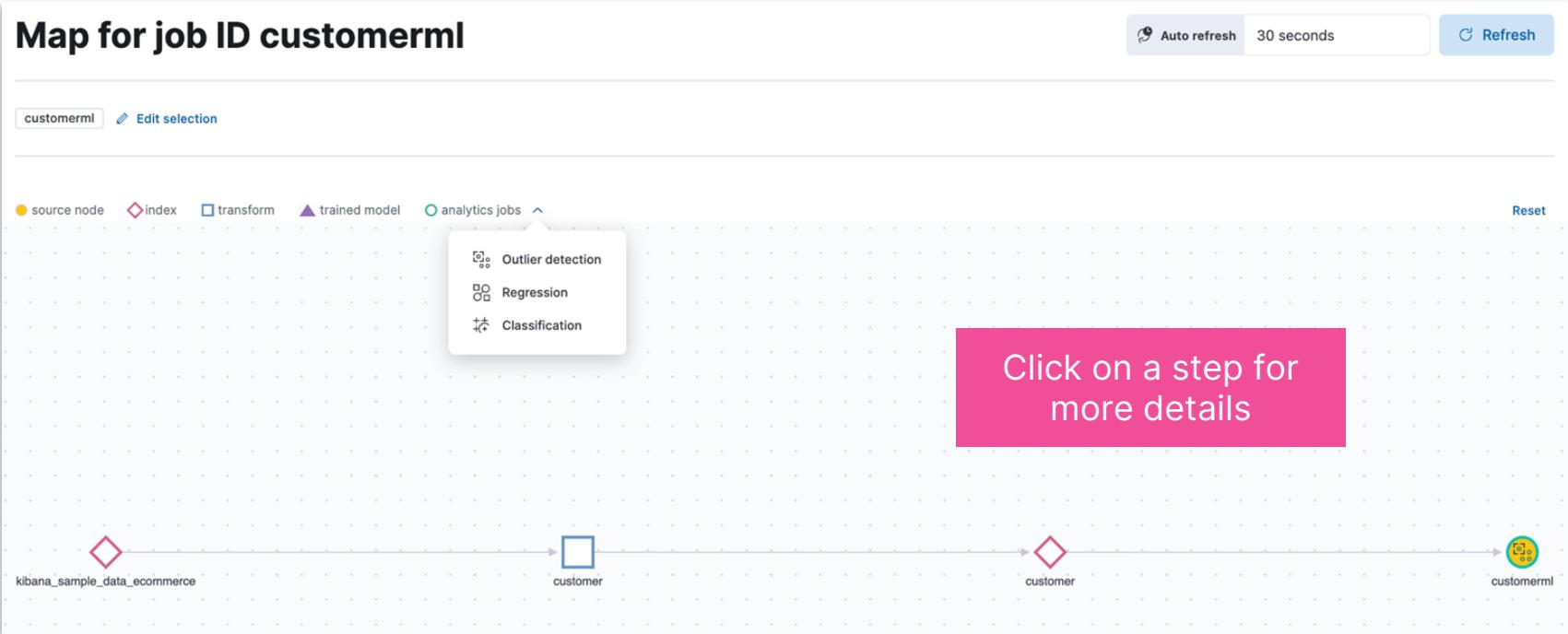
↓ ml.outlier_score	ml.feature_influence	customer_id	order_date.value_count	products.quantity.sum	taxful_total_price.sum	top_metrics.customer_full
1	[{"feature_name": "order_..."}]	27	348	878	30,787.484	Elyssa Barnes
0.603	[{"feature_name": "order_..."}]	52	188	506	17,830.453	Abd Hayes
0.326	[{"feature_name": "order_..."}]	17	170	433	14,911.75	Wilhemina St. Morrison
0.292	[{"feature_name": "order_..."}]	20		301	10,702.922	Mary James
0.24	[{"feature_name": "order_..."}]	5		409	14,160.047	Rabbia Al Hodges



Customers are given an outlier score from 0-1

Scatterplots help visualize how anomalous the data is

# Review the process



# Summary: Data frame analytics

Module 6 Lesson 3

# Summary

- Data analysis sometimes requires **transforming** event-centric time series data into entity-centric data
- Transforms can be based on **pivot** or **latest**
- **Data frame analytics** enable you to analyze entity-centric data for:
  - outlier detection
  - regression
  - classification

# Quiz

- 1. True or False:** Data frame analytics can be used for outlier detection.
- 2. True or False:** Transforms replace the original data.
3. Name two types of transforms that Elastic supports.

# Data frame analytics

Lab 6.3 - Explore data frame analytics

# AIOps Labs

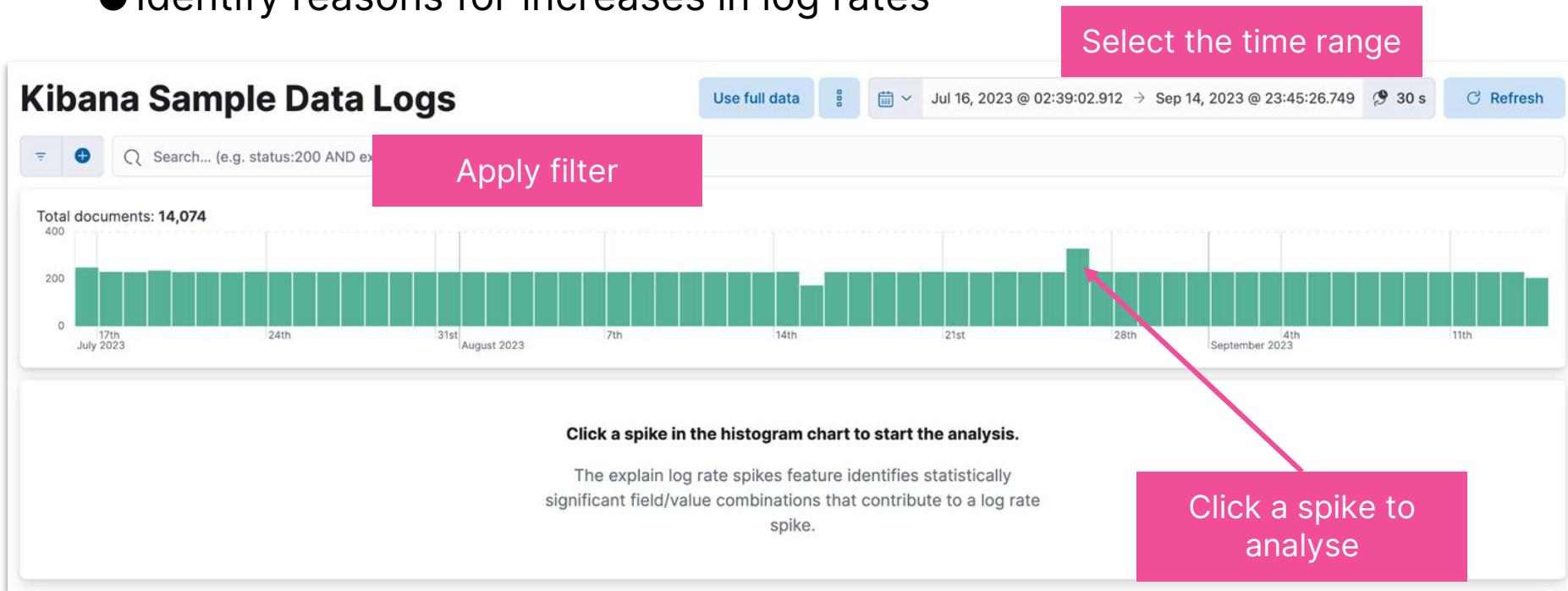
Module 6 Lesson 4

# AIOps

- Reduce the time to understand your data
- Automate IT operations by leveraging AI and machine learning
  - Explain log rate spikes
  - Log pattern analysis
  - Change point detection

# Explain log rate spikes

- Identify reasons for increases in log rates



# Explain log rate spikes

## Kibana Sample Data Logs

Use full data



Jul 16, 2023 @ 02:39:02.912 → Sep 14, 2023 @ 23:45:26.749



30 s

Refresh



Search... (e.g. status:200 AND extension:"PHP")

Total documents: 14,074

Clear selection

Baseline

Deviation

Field sorted by impact

Progress: 100% — Done.

Summarize the results into groups

Field name	Field value	Log rate	Doc count	p-value	Impact	Actions
referer	http://www.elastic-elastic-elastic.com/success/timothy-l-kopra		101	1.41e-53	High	...
clientip	30.156.16.164		100	2.81e-53	High	...
ip	30.156.16.163		101	3.09e-53	High	...
host.keyword	elastic-elastic-elastic.org		112			...
response.keyword	404		110			...
geo.dest	IN		135			...
geo.srcdest	US:IN		135			...



The spike is coming from the same IP

# Log pattern analysis

- Find patterns in unstructured log messages

### Log pattern analysis TECHNICAL PREVIEW

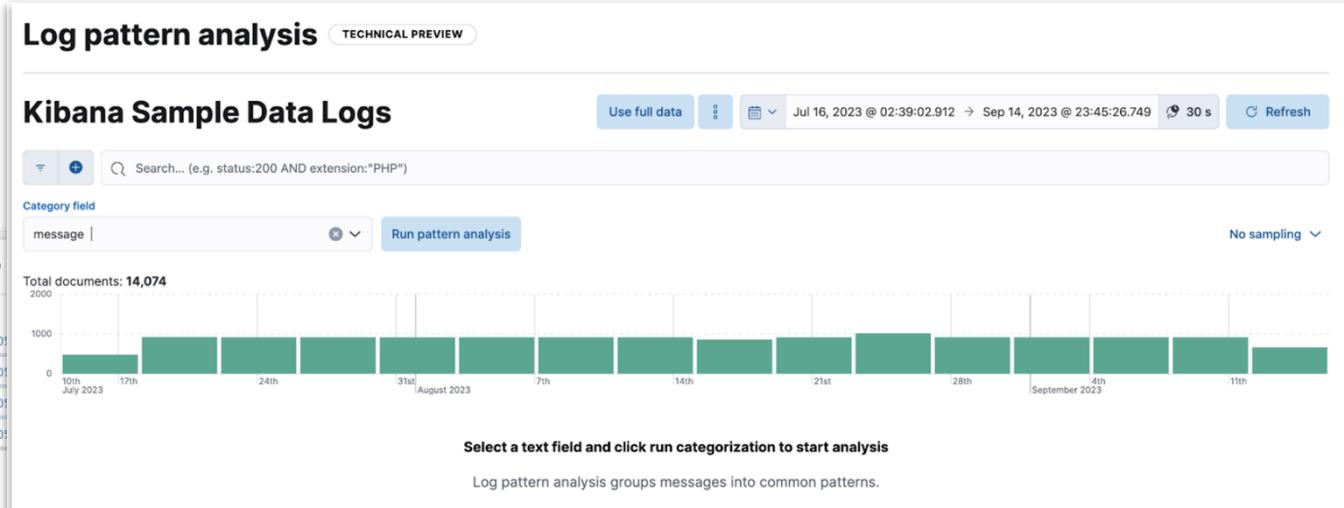
#### Kibana Sample Data Logs

Total documents: 14,074

message |

10th July 2023 17th 24th 31st August 2023 7th 14th 21st 28th 4th September 2023 11th

Select a text field and click run categorization to start analysis  
Log pattern analysis groups messages into common patterns.



Available in Discover

Visualize

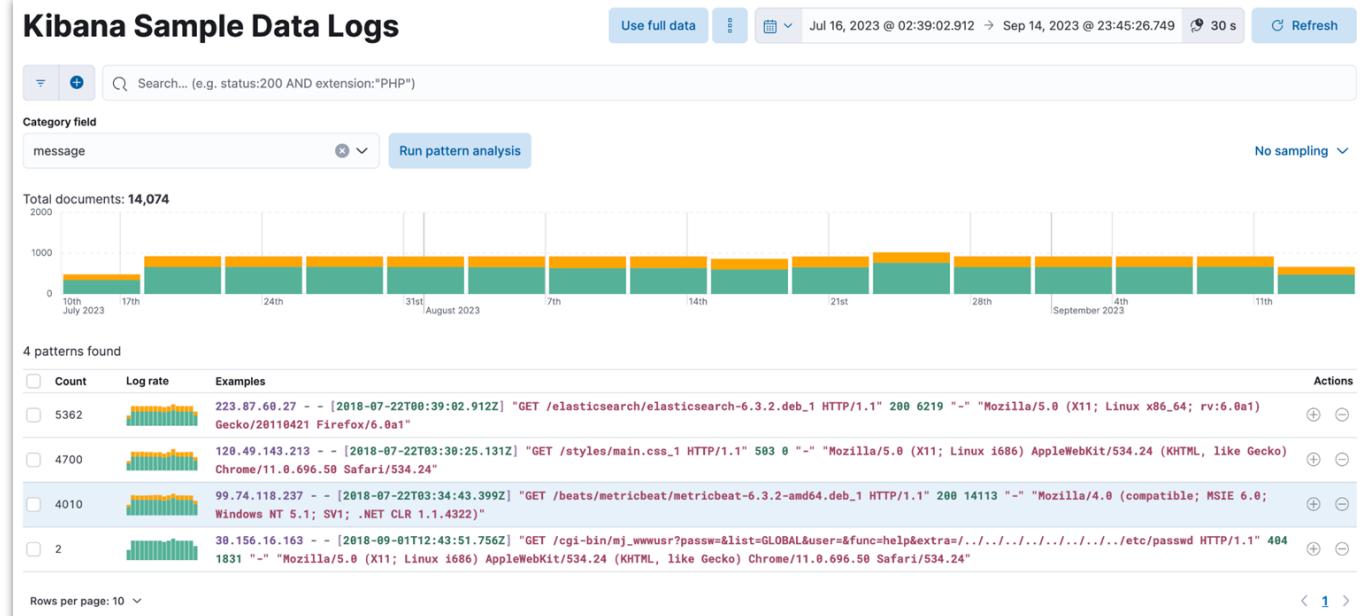
Empty fields 0 Add a field

# Log pattern analysis

Top values	
177.120.218.48 -- [2018-07-...	0.2%
0.207.229.147 -- [2018-07-2...	0.0%
0.207.229.147 -- [2018-08-0...	0.0%
0.207.229.147 -- [2018-08-0...	0.0%
0.209.144.101 -- [2018-07-2...	0.0%
0.209.144.101 -- [2018-07-3...	0.0%
0.72.176.46 -- [2018-07-23T...	0.0%
0.72.176.46 -- [2018-07-29T...	0.0%
1.145.31.121 -- [2018-07-24T...	0.0%
1.145.31.121 -- [2018-07-26T...	0.0%
Other	99.4%

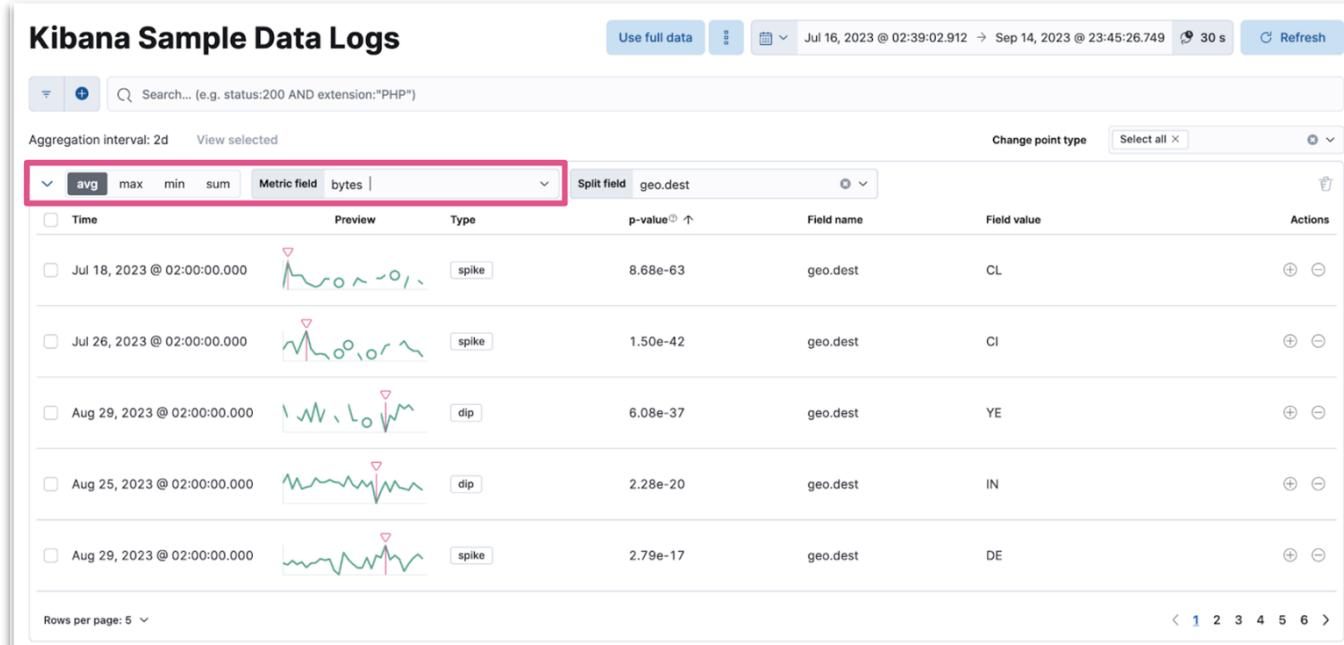
Calculated from 2,818 records.

Easier to examine unstructured data



# Change point detection

- Detect distribution or trend changes



# Summary: AIOps Labs

Module 6 Lesson 4

# Summary

- Artificial Intelligence for IT Operations (AIOps) automates IT processes by leveraging big data and machine learning
- Explain log rate spikes is a feature that identifies reasons for increases in log rates
- Log pattern analysis helps you to find patterns in unstructured log messages and makes it easier to examine your data
- Change point detection detect significant changes in a metric of your time series data

# Quiz

1. What are the three features provided by the AIOps labs?
2. Which feature would you use to detect sudden changes in your metric?
3. Is it useful to use log pattern analysis on the “country\_name” field?

# AIOps Labs

Lab 6.4 - Get insights faster

# Data Analysis with Kibana: Agenda

- Getting Started
- Search your Data
- Visualize your Data
- Additional Visualizations
- Present your Data
- Analyze your Data with Machine Learning
- **Advanced Kibana**
- Alerting

# Advanced Kibana

Module 7

# Lessons

- Formulas
- Runtime fields
- Vega

# Formulas

Module 7 Lesson 1

# Lens Formulas

- Divide two values to produce a percent
  - Metric for subset of docs over entire dataset
  - This week metric over last week metric
  - Metric for individual group over all groups

We will get back  
to this example  
soon!

Metric

Value

Method

Quick function      Formula

Formula

```
count(kql='response.keyword >= 400 and response.keyword < 500') / count()
```

Table

Kibana Sample Data Logs

Rows Optional

URL

+ Add or drag-and-drop a field

Split metrics by Optional

+ Add or drag-and-drop a field

Metrics

Visits

Unique

HTTP 4xx

HTTP 5xx

95th percentile of bytes

Median of bytes

+ Add or drag-and-drop a field



# Formulas categories

- Elasticsearch metrics
  - average, min, max, sum, etc
- Time series functions that use Elasticsearch metrics
  - cumulative\_sum,  
moving\_average, etc
- Math functions
  - abs, round, sqrt, etc

The screenshot shows a user interface for 'Formula reference'. On the left, there's a sidebar with a search bar and sections for 'How it works', 'Common formulas', and several aggregation types: 'Filter ratio', 'Week over week', 'Percent of total', and 'Recent change'. The main content area is titled 'How it works' and contains the following text:

Lens formulas let you do math using a combination of Elasticsearch aggregations and math functions. There are three main types of functions:

- Elasticsearch metrics, like `sum(bytes)`
- Time series functions use Elasticsearch metrics as input, like `cumulative_sum()`
- Math functions like `round()`

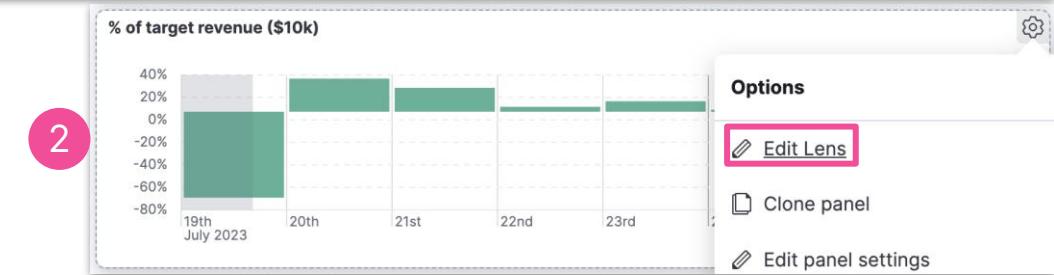
An example formula that uses all of these:

```
round(100 * moving_average(
```

# Formulas categories

1

1. Pick and edit dashboard
2. Edit lens
3. Understand context
4. Examine formula

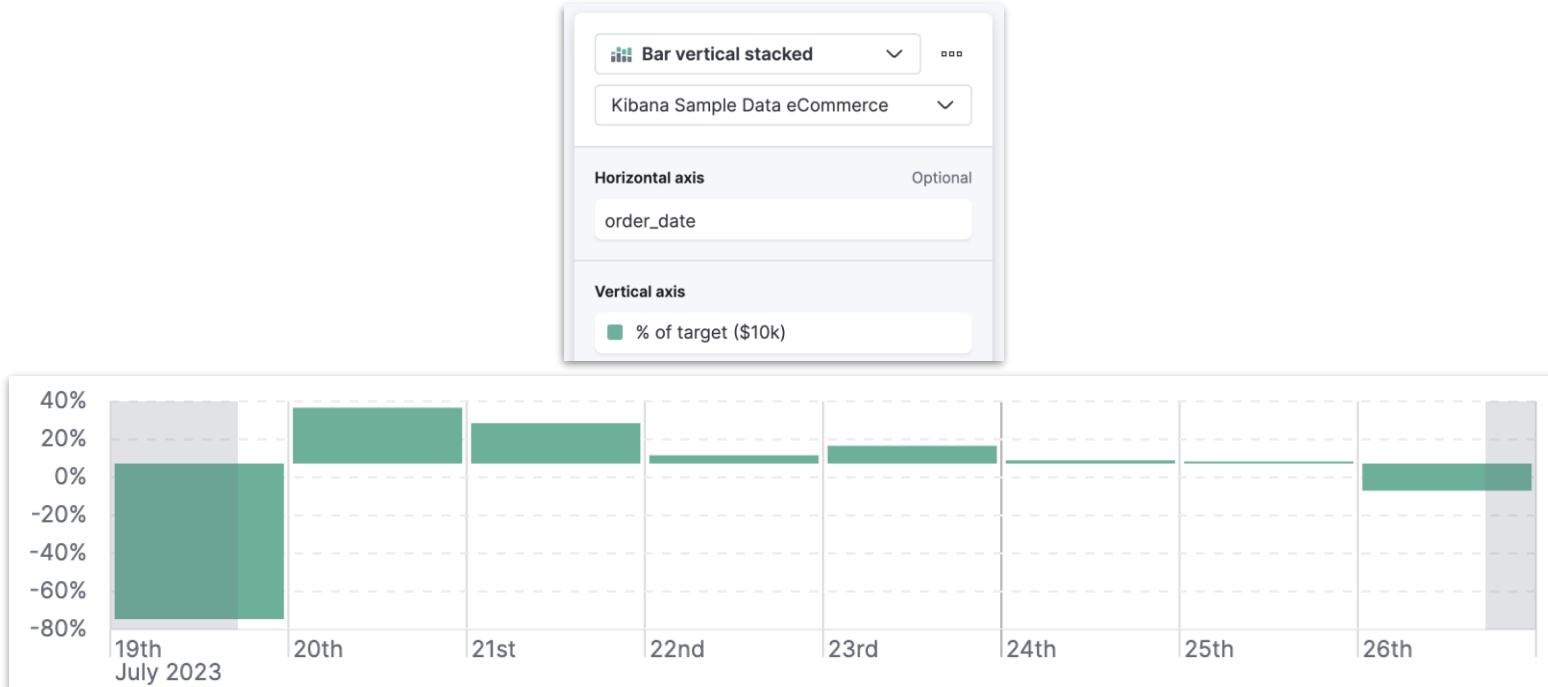


3

4

# % of target revenue (\$10k)

- [eCommerce Revenue Dashboard]



# Horizontal axis

- Groups daily orders together

Bar vertical stacked  
Kibana Sample Data eCommerce

Horizontal axis  
order\_date

Vertical axis  
% of target (\$10k)

Horizontal axis

Data

Functions Date histogram Intervals Top values

Filters

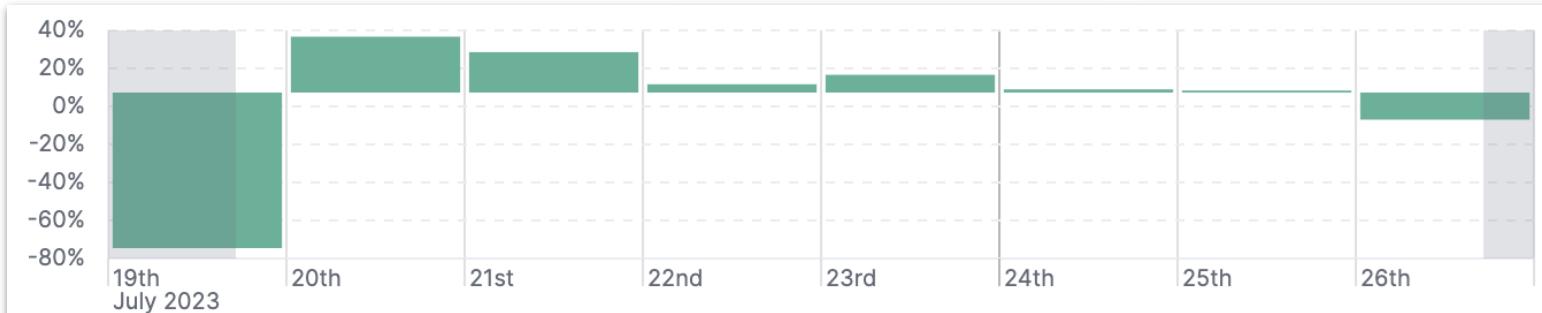
Field order\_date

Include empty rows

Minimum interval 1d

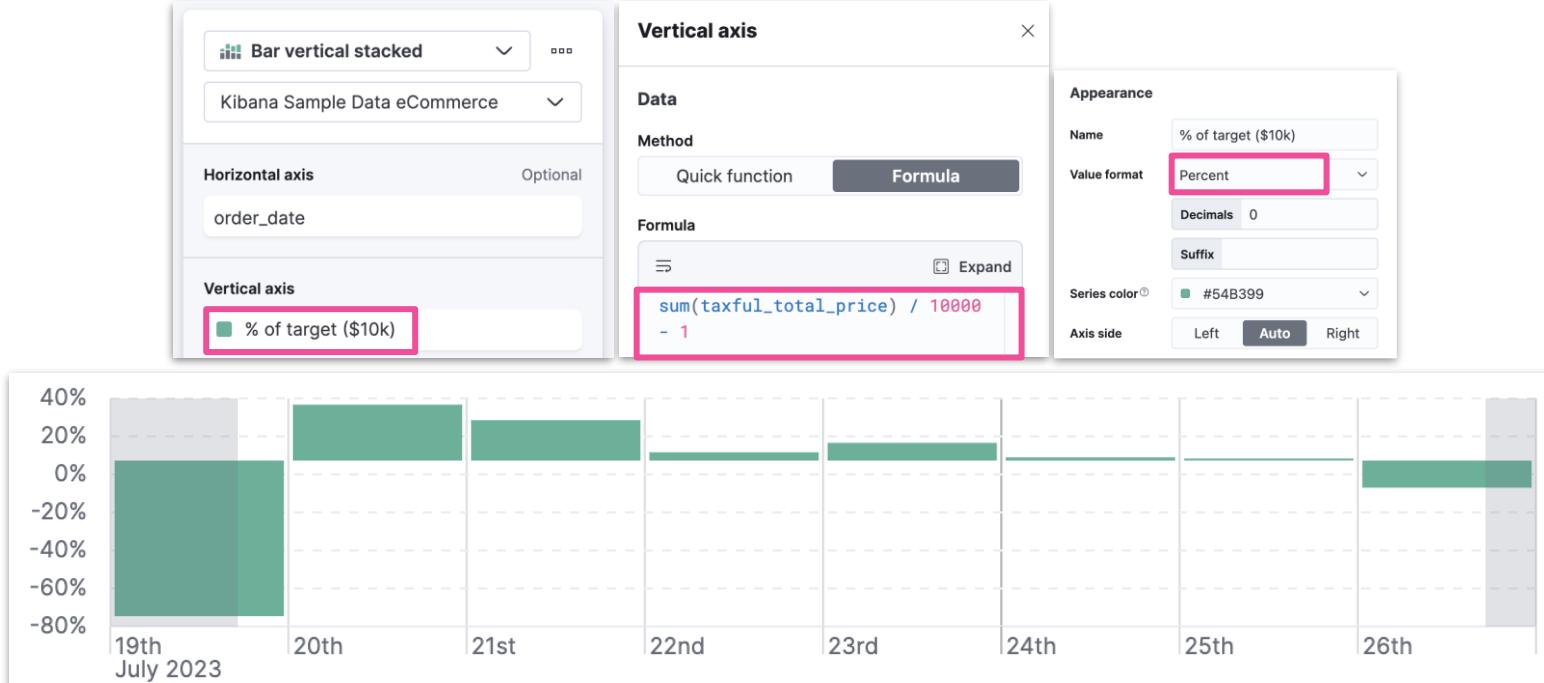
Select an option or create a custom value.  
Examples: 30s, 20m, 24h, 2d, 1w, 1M

Drop partial intervals



# Vertical axis

- Calculates total daily sales and divide by target revenue (10k)



# Daily comparison

- From [eCommerce Revenue Dashboard]

The screenshot shows the configuration interface for a 'Table' visualization in Kibana. It includes sections for 'Rows' (set to 'order\_date'), 'Split metrics by' (optional), and 'Metrics' (set to 'This week', '1 week ago', and 'Difference'). The 'Difference' metric is highlighted with a red border.

order_date per day	This week	1 week ago	Difference
2023-07-19	\$2,500.31	\$1,728.75	771.56
2023-07-20	\$12,696.16	\$10,216.38	2,479.79
2023-07-21	\$11,949.16	\$10,159.2	1,789.95

# Rows

- Group daily orders together

The screenshot shows the configuration interface for a Kibana Table visualization. The top section is titled 'Table' and has a dropdown for 'Kibana Sample Data eCommerce'. Below it, under 'Rows' (Optional), the field 'order\_date' is selected and highlighted with a pink box. Under 'Metrics' (Optional), the 'Difference' metric is selected and highlighted with a pink box. To the right, a 'Row' panel is open, showing the selected 'order\_date' field and the 'Date histogram...' function, also highlighted with a pink box. The 'Intervals' dropdown is set to '1d'.

order_date per day	This week	1 week ago	Difference
2023-07-19	\$2,500.31	\$1,728.75	771.56
2023-07-20	\$12,696.16	\$10,216.38	2,479.79
2023-07-21	\$11,949.16	\$10,159.2	1,789.95

# Difference column

- Calculates the total daily sales subtracted by total daily sales for same day a week ago

The screenshot shows the configuration for a Kibana Table visualization. The 'Table' tab is selected. In the 'Rows' section, 'order\_date' is listed as an optional field. Under 'Split metrics by', there is an optional field for adding a field to split metrics. In the 'Metrics' section, 'This week' and '1 week ago' are listed. Below them, a 'Difference' metric is selected, highlighted with a pink border. The formula for the Difference metric is shown in the 'Formula' section: `sum(taxful_total_price) - sum(taxful_total_price, shift='1w')`.

order_date per day	This week	1 week ago	Difference
2023-07-19	\$2,500.31	\$1,728.75	771.56
2023-07-20	\$12,696.16	\$10,216.38	2,479.79
2023-07-21	\$11,949.16	\$10,159.2	1,789.95

# [Logs] Errors by host

- From [Logs] Web Traffic dashboard

Table

Kibana Sample Data Logs

Rows Optional

URL  
+ Add or drag-and-drop a field

Split metrics by Optional

+ Add or drag-and-drop a field

Metrics

Visits

Unique

HTTP 4xx

HTTP 5xx

95th percentile of bytes

Median of bytes

URL

HTTP 4xx

URL	HTTP 4xx (%)
https://elastic-elastic-elastic.org/people/type:astronauts/name:klaus-dietrich-flade/profile	0.0%
https://www.elastic.co/solutions/enterprise-search	0.0%
https://www.elastic.co/products	0.0%
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm	3.4%
https://www.elastic.co/solutions/business-analytics	6.3%

# Rows

- Show top 1000 URLs by visit

Kibana Sample Data Logs

**Rows** ⚡ Optional

URL

+ Add or drag-and-drop a field

**Split metrics by** ⚡ Optional

+ Add or drag-and-drop a field

**Metrics**

Visits

Unique

HTTP 4xx

HTTP 5xx

95th percentile of bytes

Median of bytes

**Row**

Data

Functions

Date histogram  
Filters

Intervals •  
**Top values**

Fields

= url.keyword

+ Add field

Number of values

1000

Rank by ⚡

Visits

URL	HTTP 4xx
https://elastic-elastic-elastic.org/people/type:astronauts/name:klaus-dietrich-flade/profile	0.0%
https://www.elastic.co/solutions/enterprise-search	0.0%
https://www.elastic.co/products	0.0%
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm	3.4%
https://www.elastic.co/solutions/business-analytics	6.3%

# HTTP 4xx column

- Calculates the number client errors based on events with response codes between 400 and 499 as percent of total number of events

Table

Kibana Sample Data Logs

Rows<sup>②</sup> Optional

URL

+ Add or drag-and-drop a field

Split metrics by<sup>②</sup> Optional

+ Add or drag-and-drop a field

Metrics

Visits

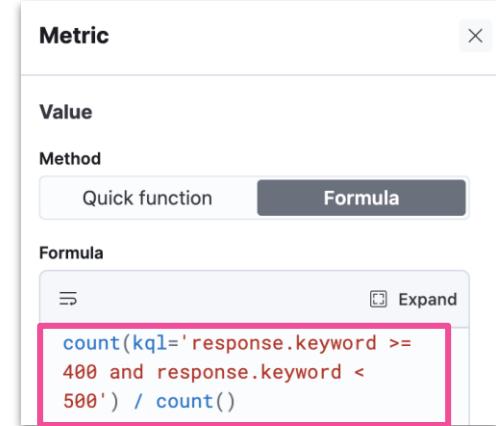
Unique

HTTP 4xx

HTTP 5xx

95th percentile of bytes

Median of bytes



URL	HTTP 4xx
https://elastic-elastic-elastic.org/people/type:astronauts/name:klaus-dietrich-flade/profile	0.0%
https://www.elastic.co/solutions/enterprise-search	0.0%
https://www.elastic.co/products	0.0%
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.3.2-i686.rpm	3.4%
https://www.elastic.co/solutions/business-analytics	6.3%

# How will you answer this?

- What percentage of daily revenue is made in the United States?



# Formula example: filter ratio

- What percentage of daily revenue is made in the United States?

The image shows three panels from a visualization tool interface:

- Horizontal axis:** Data source is "order\_date". Functions selected are "Date histogram" and "Top values". Field is "order\_date". Includes empty rows are checked. Minimum interval is set to "Day". Drop partial intervals is checked.
- Vertical axis:** Method is set to "Formula". The formula is:

```
sum(taxful_total_price,
kql='geoip.
country_iso_code:US') / sum
(taxful_total_price)
```
- Appearance:** Name is "US revenue". Value format is "Percent" with 2 decimals. Series color is "#54B399". Axis side is set to "Auto".

# Summary: Formulas

Module 7 Lesson 1

# Summary

- Formulas enable you to visualize the results of math operations on your data
- Formulas are entered in the **Formula** tab in the **Lens** editor
- Formulas can combine:
  - Elasticsearch aggregations
  - column calculations
  - math functions
- Lens provides built-in reference documentation for all functions

# Quiz

- 1. True or False:** The results of a formula can be filtered with a KQL or Lucene query.
- 2. True or False:** The results of a formula can be time shifted.
- 3. True or False:** The formula below finds the percentage of visitors to a webpage that received any error.

```
count(kql='response.keyword == 404') / count()
```

# Formulas

Lab 7.1 - Customize your visualization math

# Runtime fields

Module 7 Lesson 2

# The need for runtime fields

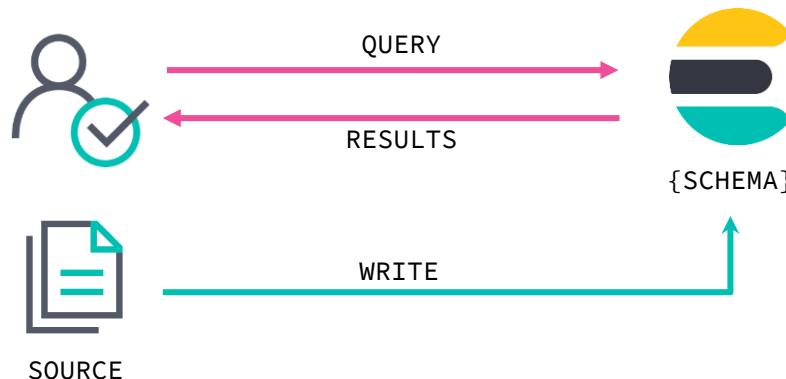
- Elasticsearch stores data in **indices**
- Kibana **queries** data stored in Elasticsearch indices
- To run **fast** queries Elasticsearch uses **structured data** by default
- There are some situations that **require** querying **unstructured data**
  - Add fields to existing documents without reindexing your data
  - Work with your data without understanding how it's structured
  - Override the value returned from an indexed field at query time
  - Define fields for a specific use without modifying its structure

# Schema on write vs on read

- Elasticsearch uses **schema on write** by default
  - All fields in a document are indexed upon ingest
- Runtime fields allow Elasticsearch to also support **schema on read**
  - Data can be quickly ingested in raw form without any indexing
  - Except for certain necessary fields such as timestamp or response codes
  - Other fields can be created on the fly when queries are run against the data

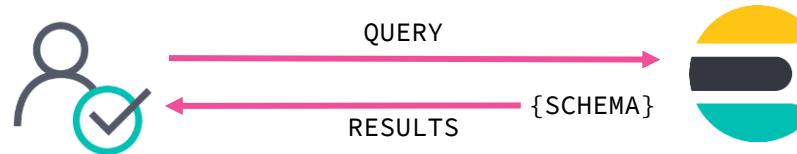
# Schema on write in detail

- Applied during data storage
- Better search performance
- Need to know data structure before writing
- Not flexible as the schema cannot be changed



# Schema on read in detail

- Applied during data retrieval
- Better write performance
- No need to know data structure before writing
- More flexible as the schema can be changed



# Runtime fields and Painless scripts

- Use Painless scripts to

- retrieve a value of fields in doc
- compute something on the fly
- to emit a value into a field

```
emit("Hello World!")
```

Return "Hello World"

```
emit(doc['bytes'].value / 1024)
```

Get byte value and return Kilobytes

```
emit(doc['timestamp'].value.getHour());
```

Get timestamp value and return the hour of the day

- Use the created field in

- queries
- visualizations

- Can impact Kibana performance

<https://www.elastic.co/guide/en/elasticsearch/painless/current/index.html>

!

# Add a runtime field

- Discover
- Lens
- Data view

The image shows two side-by-side screenshots of the Kibana interface. Both screenshots have a pink box highlighting the 'Add a field to this data view' button.

**Left Screenshot (Discover View):**

- Header: D Discover
- Data views:
  - Kibana Sample Data Logs (selected)
  - Kibana Sample Data eCommerce
  - Kibana Sample Data Flights
- Actions:
  - Add a field to this data view
  - Manage this data view
- Field list:
  - clientip
  - event.dataset
  - extension
  - geo.coordinates
  - geo.dest
  - geo.src
  - geo.srctest
  - host
  - hour\_of\_day
  - index
  - ip
  - ip\_range
  - machine.os
- Bottom: Add a field

**Right Screenshot (Data View View):**

- Header: D Discover
- Data views:
  - Kibana Sample Data Logs (selected)
  - Kibana Sample Data eCommerce
  - Kibana Sample Data Flights
- Actions:
  - Add a field to this data view
  - Manage this data view
- Summary:
  - 1,835 hits
  - Jul 20, 2023 @ 00:00:00
- Metrics:
  - Documents
  - Field statistics
- Text: Get the best look at your search results
- Bottom: Stack Management > Data views > Kibana Sample Data Logs
  - Cases
  - Connectors
  - Reporting
  - Machine Learning
  - Watcher
  - Maintenance Windows
  - Security
    - Users
    - Roles
    - API keys
    - Role Mappings
  - Kibana
    - Data Views
- Fields (44) Scripted fields (0) Field filters (0) Relationships (5)
  - Index pattern: kibana\_sample\_data\_logs Time field: timestamp
  - Fields table:

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		•	•	
_id	_id		•		
index	index		•		
  - Add field

# Create a runtime field

- Provide a name
- Define the output type

**Create field**  
Data view: Kibana Sample Data Logs

Name  Type

**Set custom label**  
Create a label to display in place of the original field in Discover, Lens, Visualize, and TSVB. Useful for fields with complex values where Queries and filters use the original field.

**Set value**  
Set a value for the field instead of retrieving it from the field with the same name in `_source`.

**Set format**  
Set your preferred format for displaying the value. Changing the format can affect the value and prevent highlighting in Discover.

[Show advanced settings](#)

[Cancel](#) [Save](#)

# Create a custom label

- Optionally customize how to display your runtime field in Kibana

**Create field**  
Data view: *Kibana Sample Data Logs*

Name	Type
response_code_definition	Keyword

**Set custom label**

Create a label to display in place of the field name in Discover, Maps, Lens, Visualize, and TSVB. Useful for shortening a long field name. Queries and filters use the original field name.

**Custom label**

Response Code Definition

# Set a value

- Define a Painless script to compute a value

 **Set value**

Set a value for the field instead of retrieving it from the field with the same name in `_source`.

**Define script**

```
1  def sc = doc['response.keyword'].value;
2  def m = ['200': 'OK', '404': 'Not Found', '503':
           'Service Unavailable', '504': 'Gateway Timeout'];
3  if (m.containsKey(sc)) {
4    emit(m[doc['response.keyword'].value])
5  }
6  else {
7    emit('None')
8 }
```

Runtime fields without a script retrieve values from `_source`. If the field doesn't exist in `_source`, a search request returns no value. [Learn about script syntax.](#)

# Set a format

- Optionally set a format to display the runtime field in the way you like

**Set format**

Set your preferred format for displaying the value. Changing the format can affect the value and prevent highlighting in Discover.

**Format (Default: String )**

String ▼

**Transform**

Upper Case ▼

**Samples**

Input	Output
A Quick Brown Fox.	A QUICK BROWN FOX.
STAY CALM!	STAY CALM!
com.organizations.project.ClassName	COM.ORGANIZATIONS.PROJECT.CLASSNAME
hostname.net	HOSTNAME.NET
SGVsbG8gd29ybGQ=	SGVSBG8GD29YBGQ=
%EC%95%88%EB%85%95%20% ED%82%A4%EB%B0%94%EB%8 2%98	%EC%95%88%EB%85%95%20% ED%82%A4%EB%B0%94%EB%8 2%98

# Preview and save

- Save your runtime field when it looks good
- You can preview any documents you want through the arrows

**Preview**  
From: kibana\_sample\_data\_logs

Document ID: mnOTk4kBqc\_oA9P-0v\_ [<](#) [>](#)

Filter fields

response_code_definition	OK
@timestamp	Sep 10, 2023 @ 06:10:01....
agent	Mozilla/5.0 (X11; Linux i68...
bytes	2,603
bytes_counter	74,023,430
bytes_gauge	2,603
clientip	49.167.60.184
event.dataset	sample_web_logs

[Show more](#)

# Notes on using runtime fields

## Benefits

- Add fields after ingest
- Does not increase index size
- Increases ingestion speed
- Readily available for use
- Promotable to indexed field

## Compromises

- Can impact search performance
  - based on script
- Index frequently searched fields
  - e.g., @timestamp
- Balance performance and flexibility
  - indexed fields + runtime fields

# Summary: Runtime fields

Module 7 Lesson 2

# Summary

- Runtime fields are Elastic's implementation of **schema on read**
- Runtime fields can be added in Kibana
  - Data Views
  - Discover
  - Lens
- To return custom values for a runtime field, you can use a script written in the Painless language
- Runtime fields are computationally expensive

# Quiz

- 1. True or False:** Runtime fields can return values that are scripted in Python or JavaScript.
- 2. True or False:** How would you return the value of a field called **my\_field** in a script?
  - a. emit(doc['my\_field'].value)
  - b. return doc['my\_field'].value
  - c. emit(myfield.value)
  - d. return myfield.value
- 3. True or False:** Runtime fields are cheap and should be used often.

# Runtime fields

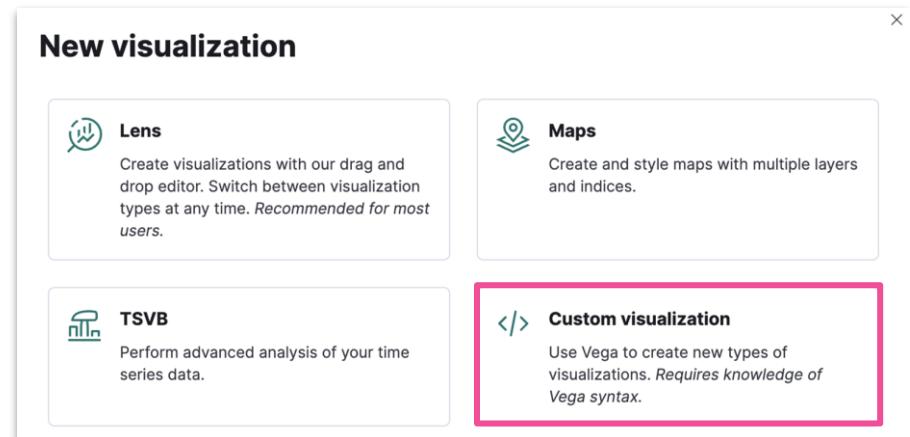
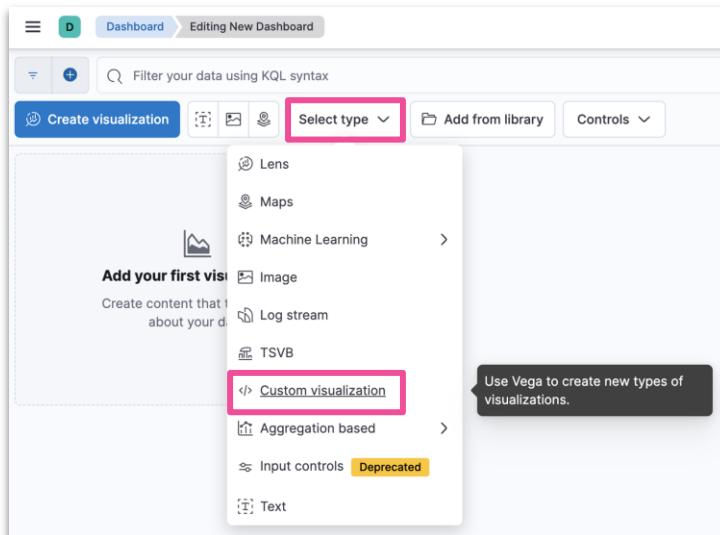
Lab 7.2 - Create a virtual field to visualize

# Vega

Module 7 Lesson 3

# Custom visualization

- What can you do to visualize data in a way that's not supported by Kibana out of the box?
- You can use **Vega** to create custom visualizations!

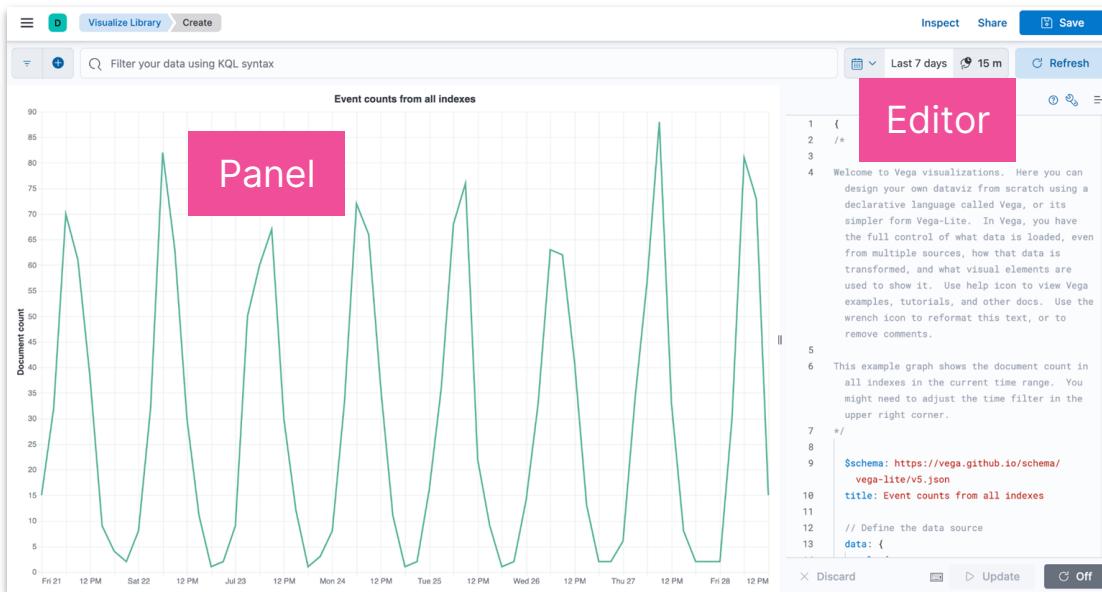


# Vega and Vega-Lite

- Vega
  - Open source visualization grammar
  - Declarative language for visualization
  - Uses JSON for describing
- Vega-Lite
  - Higher level language
  - Built on top of VEGA
  - Used to rapidly create common statistical graphics
- For simplicity, we cover Vega-Lite in this training

# Vega-Lite visualizations

- Panel can use data from
  - Elasticsearch
  - Elastic Map Service
  - URL
  - Static data
- Kibana panel supports HJSON, though both Vega-Lite and Vega use JSON



# Getting started with Vega-Lite

- Visit the Vega-Lite example gallery:  
[vega.github.io/vega-lite/examples](https://vega.github.io/vega-lite/examples)
- Select any example to see its JSON specification

The resulting visualization

The **JSON specification** for creating this visualization

Vega-Lite Examples Tutorials Documentation Usage Ecosystem GitHub Try Online

## Simple Bar Chart

A bar chart encodes quantitative values as the extent of rectangular bars.

Category	Value
A	28
B	55
C	43
D	91
E	81
F	53
G	19
H	87
I	52

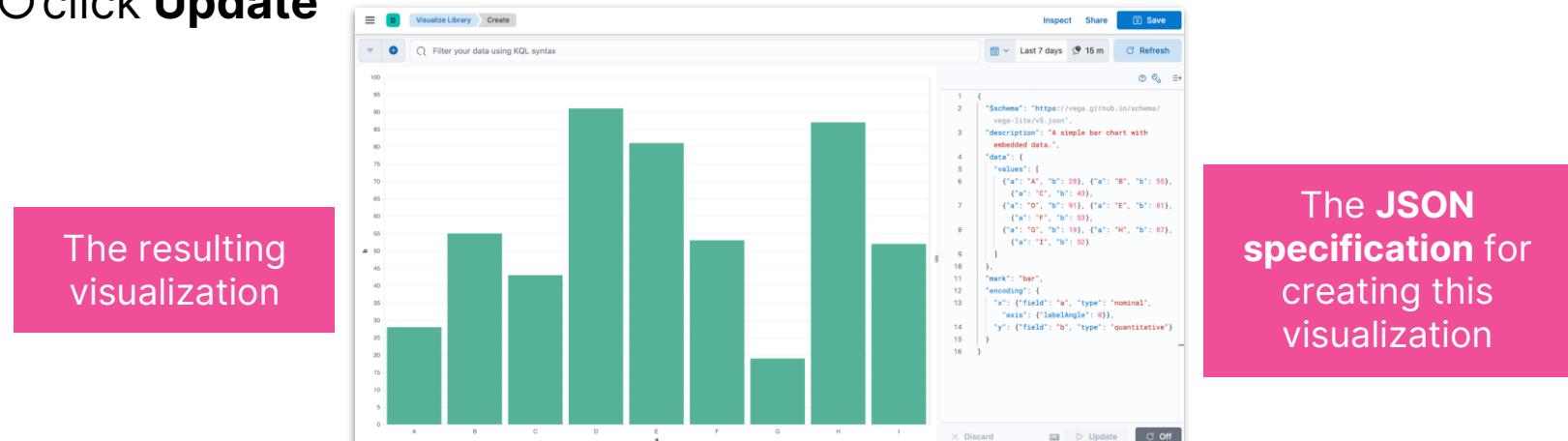
[View this example in the online editor](#)

### Vega-Lite JSON Specification

```
{ "schema": "https://vega.github.io/schema/vega-lite/v5.json", "description": "A simple bar chart with embedded data.", "data": { "values": [ {"a": "A", "b": 28}, {"a": "B", "b": 55}, {"a": "C", "b": 43}, {"a": "D", "b": 91}, {"a": "E", "b": 81}, {"a": "F", "b": 53}, {"a": "G", "b": 19}, {"a": "H", "b": 87}, {"a": "I", "b": 52} ] }, "mark": "bar", "encoding": { "x": {"field": "a", "type": "nominal", "axis": {"labelAngle": 0}}, "y": {"field": "b", "type": "quantitative"} } }
```

# Creating a custom Vega-Lite visualization

- To see the visualization in Vega or Vega-Lite in Kibana
  - **copy** the JSON specification of a Vega-Lite example
  - create a new **custom visualization** in Kibana
  - **paste** the specification in the editor
  - click **Update**



# Let's take a look at the bar chart specification

```
{  
  "$schema": "https://vega.github.io/schema/vega-lite/v5.json",  
  "description": "A simple bar chart with embedded data.",  
  "data": {  
    "values": [  
      {"a": "A", "b": 28},  
      {"a": "B", "b": 55},  
      {"a": "C", "b": 43},  
      {"a": "D", "b": 91},  
      {"a": "E", "b": 81},  
      {"a": "F", "b": 53},  
      {"a": "G", "b": 19},  
      {"a": "H", "b": 87},  
      {"a": "I", "b": 52}  
    ]  
  },  
  "mark": "bar",  
  "encoding": {  
    "x": {"field": "a", "type": "nominal", "axis": {"labelAngle": 0}},  
    "y": {"field": "b", "type": "quantitative"}  
  }  
}
```

The **data** to visualize. Can be embedded as values, or retrieved from Elasticsearch

**mark** defines the type of chart. Can be **line**, **bar**, **area**, etc.

How to **encode** the data to **x**, **y** or **color**

# Retrieve data from Elasticsearch

- Use the **data** clause to retrieve data from Elasticsearch
- specify a **url** clause with a **%timefield%**, **index**, and **body**
- and a **format** clause with a **property**

```
"data": {  
  "url": {  
    "%timefield%": "...",  
    "index": "...",  
    "body": {  
      ...  
    }  
  },  
  "format": {  
    "property": "..."  
  }  
}
```

The **timefield** used by the time filter

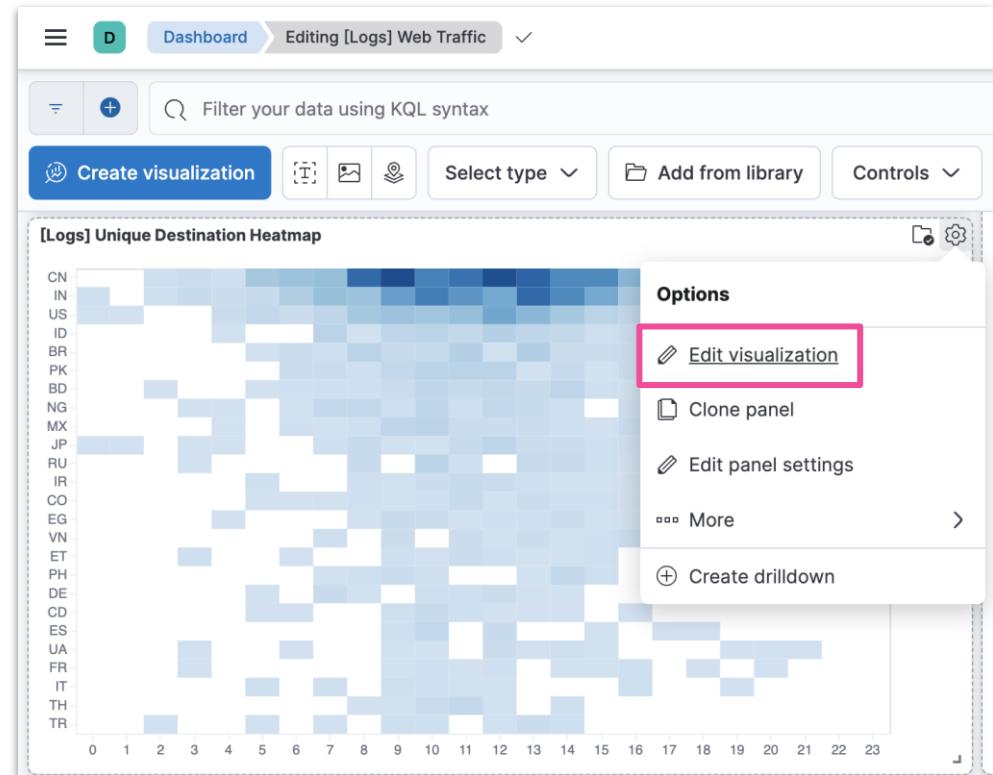
Index or **indices** from which you want to retrieve data

The **body** of a request to Elasticsearch (covered in **Elasticsearch Engineer**)

The **property** in the response you want to visualize

# Vega-Lite in sample dashboards

- Color intensity shows the number of unique visitors
- X-axis shows daily hours
- Y-axis shows countries



# Editing the sample visualization

- You can check the JSON used to create the custom visualization

```
$schema: "https://vega.github.io/schema/vega-lite/v5.json"
data: {
  url: {
    %context%: true
    $timefield$: @timestamp
    index: kibana_sample_data_logs
  }
}
body: {
  aggs: {
    countries: {
      terms: {
        field: geo.dest
        size: 25
      }
    }
    aggs: {
      hours: {
        histogram: {
          field: hour_of_day
          interval: 1
        }
      }
      aggs: {
        unique: {
          cardinality: {
            field: clientip
          }
        }
      }
    }
  }
}
```

The **url** clause uses the **kibana\_sample\_data\_logs** index and keeps the Dashboard context

# Body example

Don't give me any actual documents as results

```
body: {  
    aggs: {  
        countries: {  
            terms: {  
                field: geo.dest  
                size: 25  
            }  
        aggs: {  
            hours: {  
                histogram: {  
                    field: hour_of_day  
                    interval: 1  
                }  
            aggs: {  
                unique: {  
                    cardinality: {  
                        field: clientip  
...  
size: 0  
    }
```

First group by top 25 destination countries

Then group by every hour of the day

Finally calculate the number of unique visitors

# Transform example

```
transform: [
  {
    flatten: ["hours.buckets"],
    as: ["buckets"]
  },
  {
    filter: "datum.buckets.unique.value > 0"
  }
]

mark: {
  type: rect
  tooltip: {
    expr: "{
      \"Unique Visitors\": datum.buckets.unique.value,
      \"geo.src\": datum.key,
      \"Hour\": datum.buckets.key}"
  }
}
```

Extract the inner array

Filter for non-zero buckets

Draw rectangles to depict cells in heatmap with tooltip

# Encoding example

```
encoding: {  
  x: { ... },  
  y: { ... },  
  color: { ... },  
}
```

```
x: {  
  field: buckets.key  
  type: nominal  
  scale: {  
    domain: {  
      expr: "sequence(0, 24)"  
    }  
  }  
  axis: {  
    title: false  
    labelAngle: 0  
  }  
}
```

Feed destination  
countries grouping to  
x-axis

```
y: {  
  field: key  
  type: nominal  
  sort: {  
    field: -buckets.unique.value  
  }  
  axis: {title: false}  
}
```

Feed hour of the day  
grouping to y-axis

```
color: {  
  field: buckets.unique.value  
  type: quantitative  
  axis: {title: false}  
  scale: {  
    scheme: blues  
  }  
}
```

Feed number of  
unique visitors  
(clientip) to color  
intensity

# Editing the sample visualization

- Relies on **tokens** to render data dynamically based on Dashboard filters

```
url: {  
  ...  
  %timefield%: @timestamp  
  ...  
  %context%: true  
  index: ...  
  body: {  
    ...  
    range: {  
      @timestamp: {  
        ...  
        "%timefilter%": true  
        ...  
    }  
}
```

Specify the time filter

Apply dashboard context filters when set

"%timefilter%" will be replaced with the current values of the time filter

# Summary: Vega

Module 7 Lesson 3

# Summary

- **Vega visualizations** are a type of visualization in Kibana, based on the open source Vega project
- Vega visualizations allow you to build visualizations using a **JSON-based grammar**
- Kibana supports **Vega** and **Vega-Lite** grammars

# Quiz

- 1. True or False:** To retrieve data from Elasticsearch you need to add an **url** and **format** clause to the **data** clause of a Vega-Lite specification.
- 2. True or False:** Vega visualizations can be added to a dashboard like any other visualization.
- 3. True or False:** A filter on a dashboard that has a Vega visualization cannot affect the Vega visualization.

# Vega

Lab 7.3 - Advanced code-based  
visualizations

# Data Analysis with Kibana: Agenda

- Getting Started
- Search your Data
- Visualize your Data
- Additional Visualizations
- Present your Data
- Analyze your Data with Machine Learning
- Advanced Kibana
- **Alerting**

# Alerting

Module 8

# Lessons

- Rules and Connectors
- Creating in-app alerts
- Managing alerts

# Rules and Connectors

Module 8 Lesson 1

# Alerting

- Define rules

- detect complex conditions
- trigger actions with built-in connectors

- Integrated with

- Observability

- Security

- Maps

- Machine Learning

**Create rule**

Name  
Kibana sites - high egress

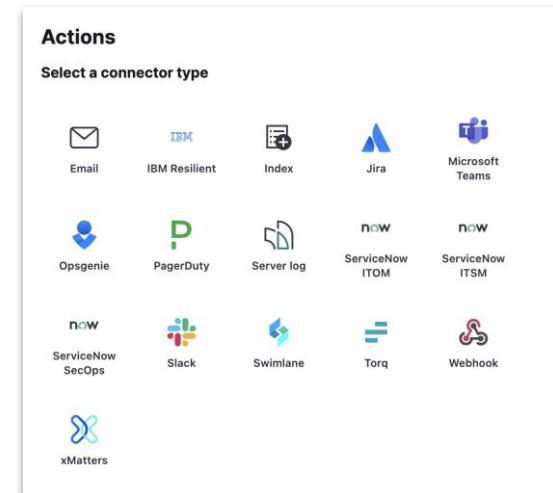
Tags (optional)

**Index threshold**  
Alert when an aggregated query meets the threshold. [Learn more](#)

INDEX kibana\_sample\_data\_logs  
WHEN sum()  
OF bytes  
GROUPED OVER top 4 'host.keyword'

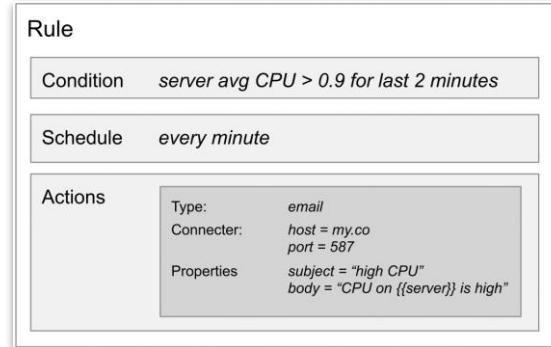
**Define the condition**  
IS ABOVE 42000

Cancel

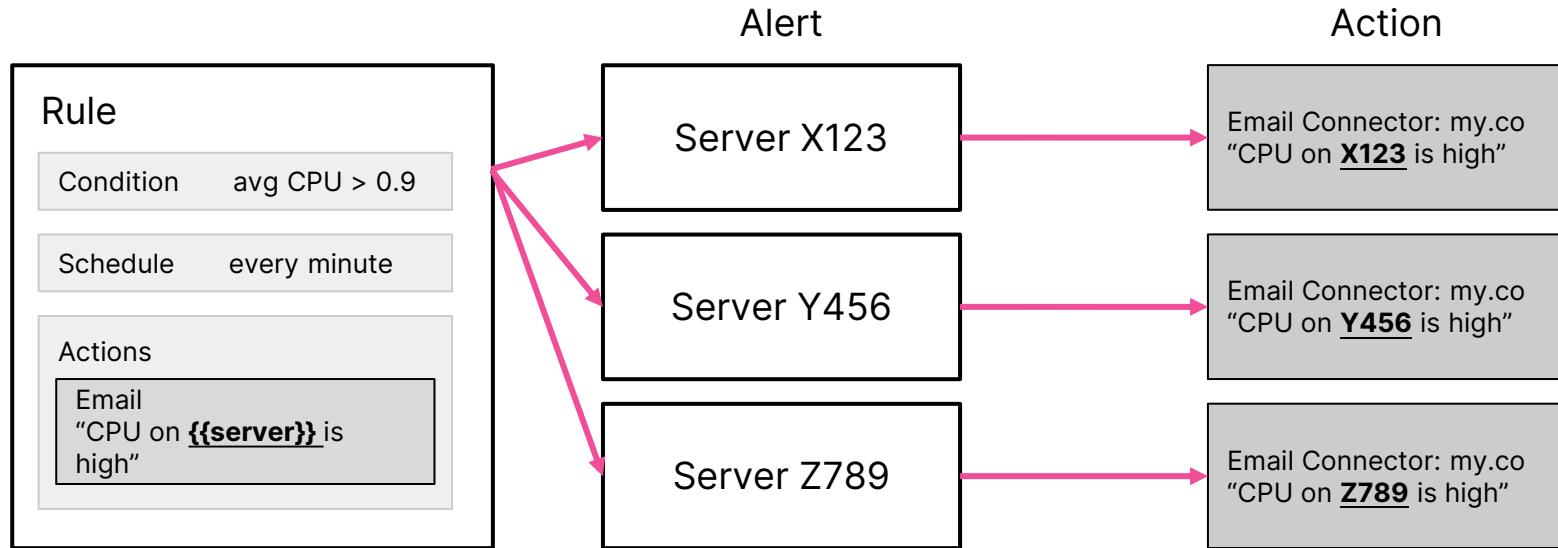


# Anatomy of rules

- Alerting works by running checks on a **schedule** to detect **conditions** defined by **a rule**
- When a condition is met, the rule tracks it as **an alert** and responds by triggering one or more **actions**
- **Actions** typically involve interaction with Kibana services or third party integrations



# Rules vs Alerts



# Connectors

- Actions often involve connecting with services inside Kibana or integrating with third-party systems
- **Connectors** provide a central place to store connection information for services and integrations



# Getting started

- Create generic rules through the **Alerts and Insights** section
- More specific rules must be created within the context of a Kibana app (we will cover in the next lesson)

The screenshot shows the Elasticsearch Stack Management interface. The left sidebar has a 'Management' heading and links for Ingest (Ingest Pipelines, Logstash Pipelines), Data (Index Management, Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Cross-Cluster Replication, Remote Clusters, Migrate), and Alerts and Insights (Rules, Cases, Connectors, Reporting, Machine Learning, Watcher, Maintenance Windows). The 'Rules' link is highlighted with a pink box. The main content area is titled 'Rules' and contains the sub-instruction 'Detect conditions using rules.' Below this are tabs for 'Rules' (selected) and 'Logs'. A central callout box says '(o)' and 'Create your first rule'. It explains: 'Receive an alert through email, Slack, or another connector when a condition is met.' A blue 'Create rule' button is at the bottom of the box. At the top right of the main content area are 'Documentation', 'Settings', and another 'Create rule' button.

# Create a rule

- Click **Create rule** to start creating one alerting rule

The screenshot shows the 'Rules' section of the Elasticsearch interface. At the top right, there are three buttons: 'Documentation', 'Settings', and a blue button with a plus sign labeled 'Create rule', which is highlighted with a pink rectangle. Below these, there are two tabs: 'Rules' (which is underlined in blue) and 'Logs'. In the center, a large white box contains a smiling face icon and the text 'Create your first rule'. Below this, it says 'Receive an alert through email, Slack, or another connector when a condition is met.' At the bottom of this box is another blue 'Create rule' button with a plus sign, also highlighted with a pink rectangle.

Rules

Documentation Settings **Create rule**

Rules Logs

(((o)))

**Create your first rule**

Receive an alert through email, Slack, or another connector when a condition is met.

**Create rule**

# Set a name

- Set a name and optionally set a tag

## Create rule

**Name**

Kibana site - high egress

**Tags (optional)**

sample-data ×

# Select a rule type

- Depending upon the context, you might be prompted to choose the type of rule to create
- Some apps will pre-select the type of rule for you

The image displays two side-by-side 'Create rule' dialog boxes from the Elasticsearch interface.

**Left Dialog (Select rule type):**

- Search bar: Search
- Filter by use case: 0
- Category: APM AND USER EXPERIENCE (4 items)
- Items:
  - Anomaly**: Alert when either the latency, throughput, or failed transaction rate of a service is anomalous.
  - Error count threshold**: Alert when the number of errors in a service exceeds a defined threshold.
  - Failed transaction rate threshold**: Alert when the rate of transaction errors in a service exceeds a defined threshold.
  - Latency threshold**: Alert when the latency of a specific transaction type in a service exceeds a defined threshold.
- Category: LOGS (1 item)
- Item: **Log threshold**: Alert when the log aggregation exceeds the threshold.

**Right Dialog (Create rule):**

- Name: Kibana site - high egress
- Tags (optional): sample-data
- Search bar: index
- Filter by use case: 0
- Category: STACK RULES (1 item)
- Item: **Index threshold**: Alert when an aggregated query meets the threshold.

# Define a condition

- Each rule type provides its own way of defining the conditions
- An expression formed by a series of clauses is a common pattern

**Create rule**

**Index threshold**  
Alert when an aggregated query meets the threshold. [Learn more](#)

**Select an index**

```
INDEX kibana_sample_data_logs  
WHEN sum()  
OF bytes
```

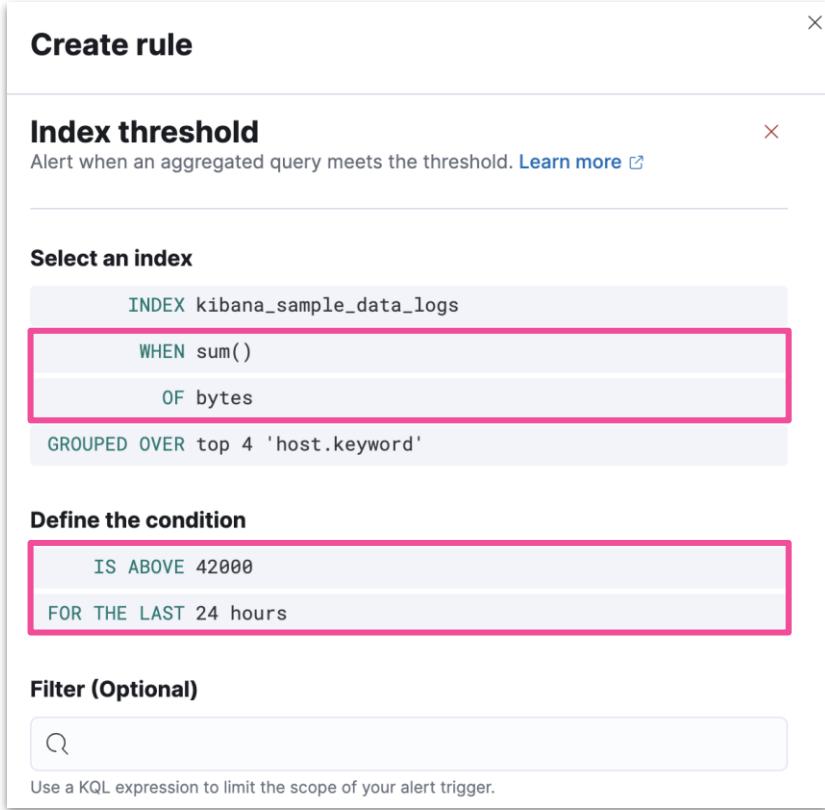
GROUPED OVER top 4 'host.keyword'

**Define the condition**

```
IS ABOVE 42000  
FOR THE LAST 24 hours
```

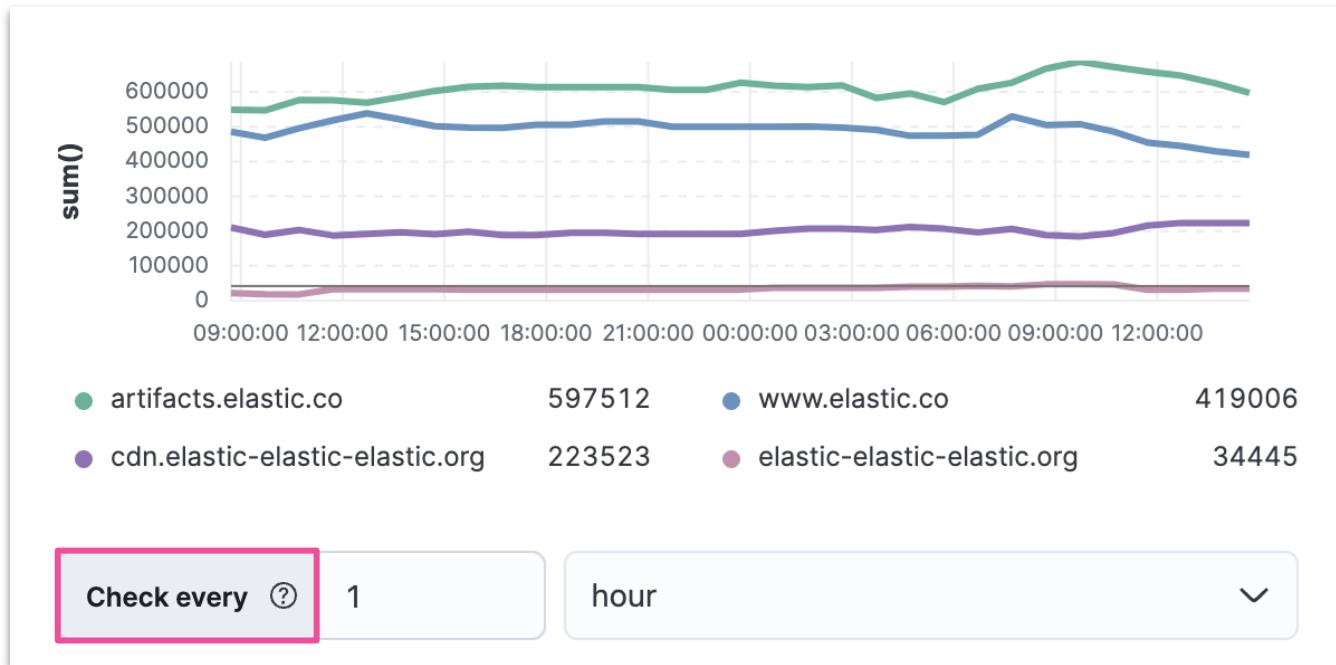
**Filter (Optional)**

Use a KQL expression to limit the scope of your alert trigger.



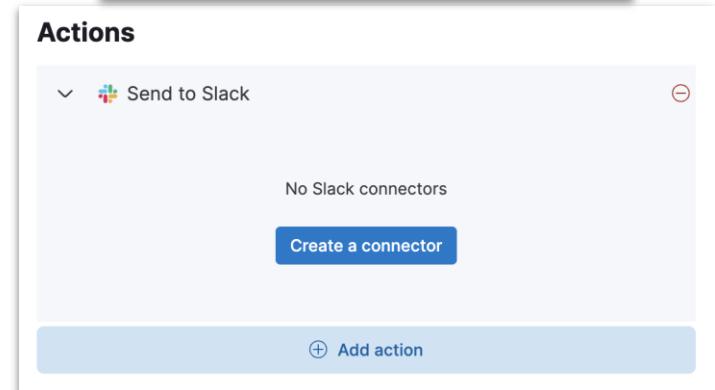
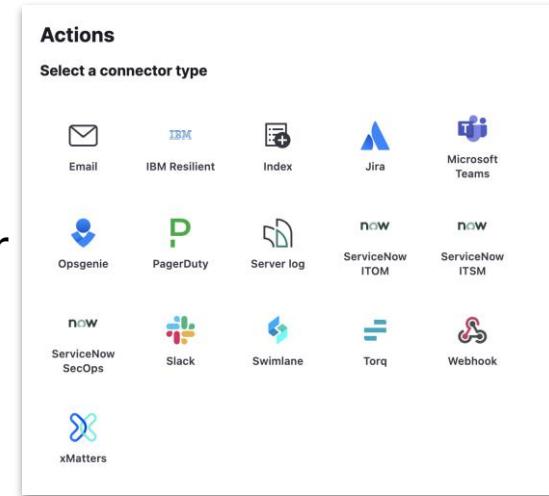
# Preview the condition

- Define how often to evaluate the condition



# Add one or more actions

- To receive notifications when a rule meets the defined conditions, you must add one or more actions
- Extend your alerts by connecting them to actions that use built-in integrations
- Each action must specify a connector
- If no connectors exists, create one



# Configure the action and connector

- Each action type exposes different properties
- For example, an email action allows you to set the recipients, the subject, and a message body in markdown format
- After you configure your actions you can save the rule

### Create rule

#### Actions

Demo emails (preconfigured)

Email connector Add connector  
Demo emails

Action frequency  
On status changes

Run when Threshold met

To  
demo@elastic.co

Cc Bcc

Subject  
Alert {{rule.name}} - site: {{context.group}} - value: {{context.value}}

Message

```
alert '{{alertName}}' is active for group '{{context.group}}':  
- Value: {{context.value}}  
- Conditions Met: {{context.conditions}} over {{params.timeWindowSize}}  
{{params.timeWindowUnit}}  
- Timestamp: {{context.date}}
```

Add action

Cancel Save

# Managing your rules

- After your rules are created you can manage them through Kibana

The screenshot shows the Kibana Management interface for 'Rules'. The left sidebar includes sections for Ingest (Ingest Pipelines, Logstash Pipelines), Data (Index Management, Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Cross-Cluster Replication, Remote Clusters, Migrate), and Alerts and Insights (Cases, Connectors, Reporting, Machine Learning, Watcher, Maintenance Windows). The main area is titled 'Rules' and displays a summary: 'Succeeded: 1 • Failed: 0 • Warning: 0'. It lists one rule named 'Kibana site - high egr', which was last run on Aug 1, 2023, at 15:03:32pm. The rule has an index threshold of 1 and is currently enabled. The table columns include Name, Last run, Notify, Int..., Duration, P50, Success rate, Last response, and State.

Name	Last run	Notify	Int...	Duration	P50	Success rate	Last response	State
Kibana site - high egr	Aug 1, 2023 Index threshold 15:03:32pm a few seconds ago	1	hr	00:01	00:01	100%	Succeeded	Enabled

# Managing your connectors

- You can also manage the connectors available for creating new rules

The screenshot shows the Elasticsearch Stack Management interface. The left sidebar has a 'Management' section with 'Ingest', 'Data', 'Alerts and Insights', and a 'Connectors' section which is highlighted with a pink rectangle. Below these are 'Reporting', 'Machine Learning', 'Watcher', and 'Maintenance Windows'. The main area is titled 'Connectors' and contains the sub-instruction 'Connect third-party software with your alerting data.' It features tabs for 'Connectors' (which is selected) and 'Logs'. A 'Create connector' button is at the top left, followed by a search bar and a 'Type' dropdown. A table lists one connector: 'Demo emails' (Type: Email, Compatibility: Alerting Rules, Status: PRECONFIGURED). At the bottom are pagination controls for 'Rows per page: 10' and navigation arrows.

# Watcher

- Can also be used to detect conditions and trigger actions in response
- It's a different alerting system though (not covered in this training)
- The scheduled checks for Watcher are run on Elasticsearch instead of Kibana
- Please refer to the docs for more differences
  - <https://www.elastic.co/guide/en/kibana/current/alerting-getting-started.html#alerting-concepts-differences>

# Summary: Rules and Connectors

Module 8 Lesson 1

# Summary

- Alerting allows you to define rules to detect complex conditions within different Kibana apps and trigger actions when those conditions are met
- You can use actions to connect with services inside Kibana or integrate them with supported third-party systems
- Alerting and Watcher are both used to detect conditions and can trigger actions in response, but they are completely independent alerting systems

# Quiz

1. What are the three building blocks of rules?
  - a. Conditions
  - b. Connector
  - c. Schedule
  - d. Actions
2. **True or False:** If I have 4 rules that send email notifications as an action, I need to create a separate connector for each one of them.
3. **True or False:** Scheduled checks for Watcher are run on Kibana.

# Rules and Connectors

Lab 8.1 - Create a rule

# Creating in-app alerts

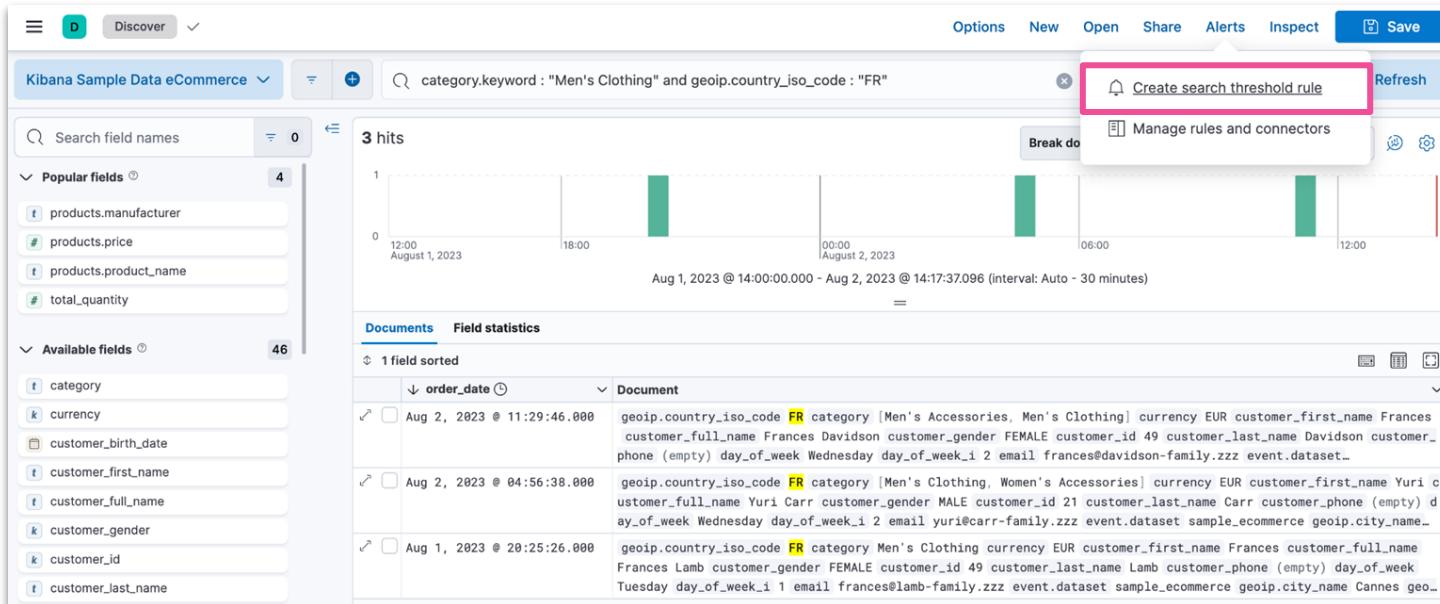
Module 8 Lesson 2

# Integrations with Kibana apps

- Alerting allows rich integrations across various Kibana apps
  - Discover
  - Maps
  - Machine Learning
  - Observability
  - Security
  - and more...

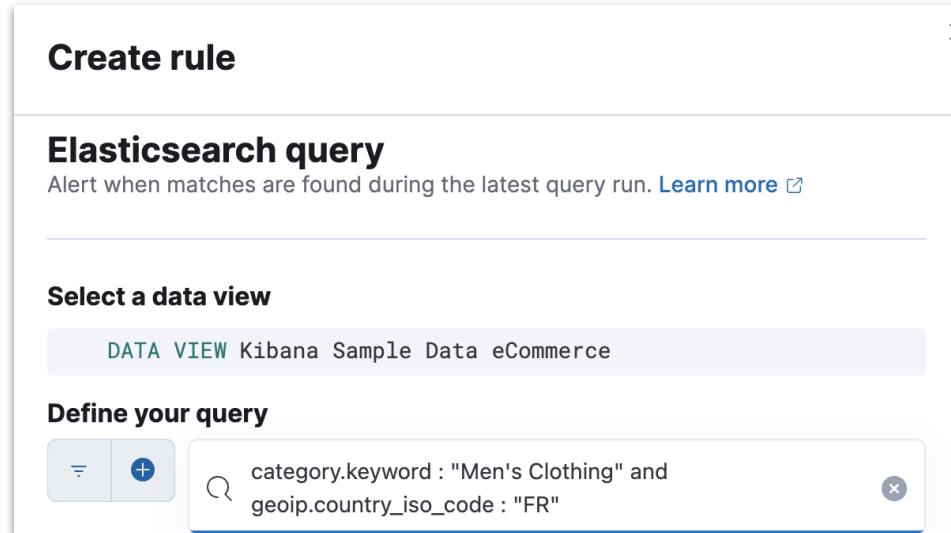
# Alerting in Discover

- Create a rule to periodically check when data goes above or below a certain threshold within a given time interval



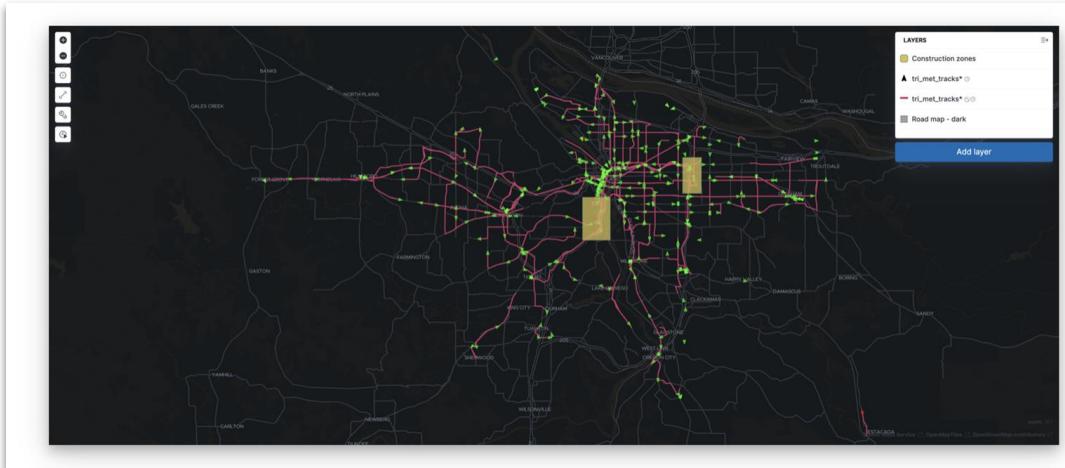
# Alerting in Discover

- Ensure that your data view, query, and filters fetch the data for which you want an alert
- The form is pre-filled with the query present in the query bar



# Alerting in Maps

- Maps offers the **Tracking containment** rule type
- It runs an Elasticsearch query over indices
- The point is to determine whether any documents are currently contained within any boundaries from the specified boundary index



# Tracking containment requirements

- Tracks index or data view
- Boundaries index or data view

**Select entity**

**INDEX** Select a data view and geo point field ⚠

**BY** Select entity field

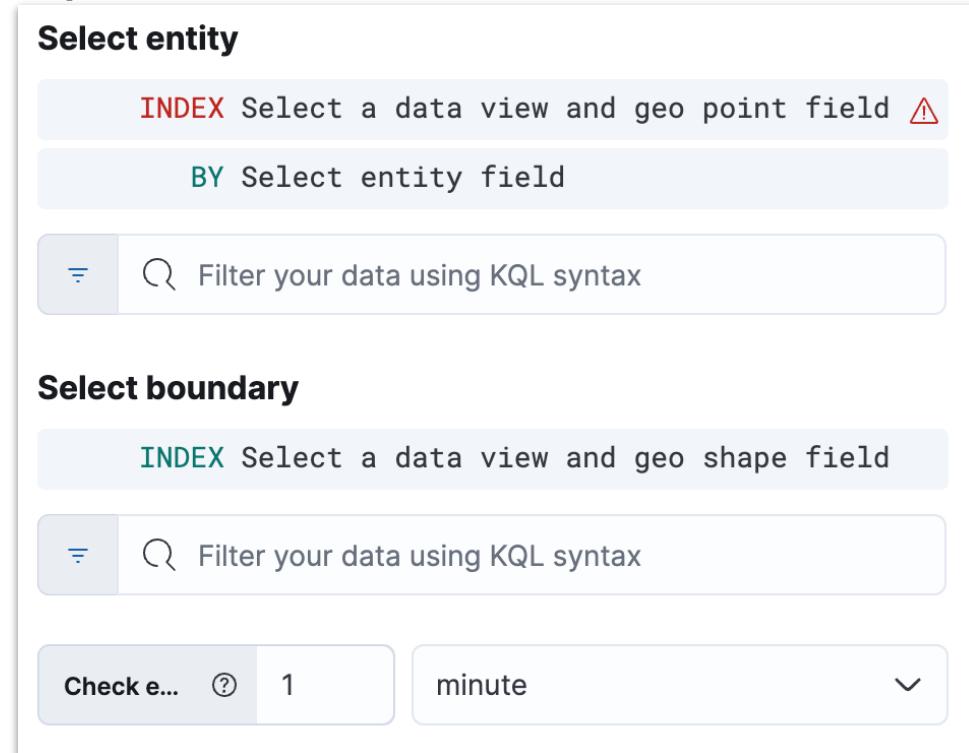
**=** Filter your data using KQL syntax

**Select boundary**

**INDEX** Select a data view and geo shape field

**=** Filter your data using KQL syntax

**Check e...** ? 1 minute ▼

The screenshot shows a configuration interface for tracking containment requirements. It is divided into two main sections: 'Select entity' and 'Select boundary'.  
  
Under 'Select entity':

- A button labeled 'INDEX' with the sub-instruction 'Select a data view and geo point field' and a red warning icon.
- A button labeled 'BY' with the sub-instruction 'Select entity field'.
- A search bar with a filter icon and the placeholder 'Filter your data using KQL syntax'.

  
  
Under 'Select boundary':

- A button labeled 'INDEX' with the sub-instruction 'Select a data view and geo shape field'.
- A search bar with a filter icon and the placeholder 'Filter your data using KQL syntax'.

  
  
At the bottom, there is a section for setting a check interval:

- A button labeled 'Check e...' with a question mark icon.
- A text input field containing the number '1'.
- A dropdown menu with the word 'minute' selected.
- A downward arrow icon indicating more options.

# Defining an action

- Conditions for how a rule is tracked can be specified uniquely for each individual action

Action frequency

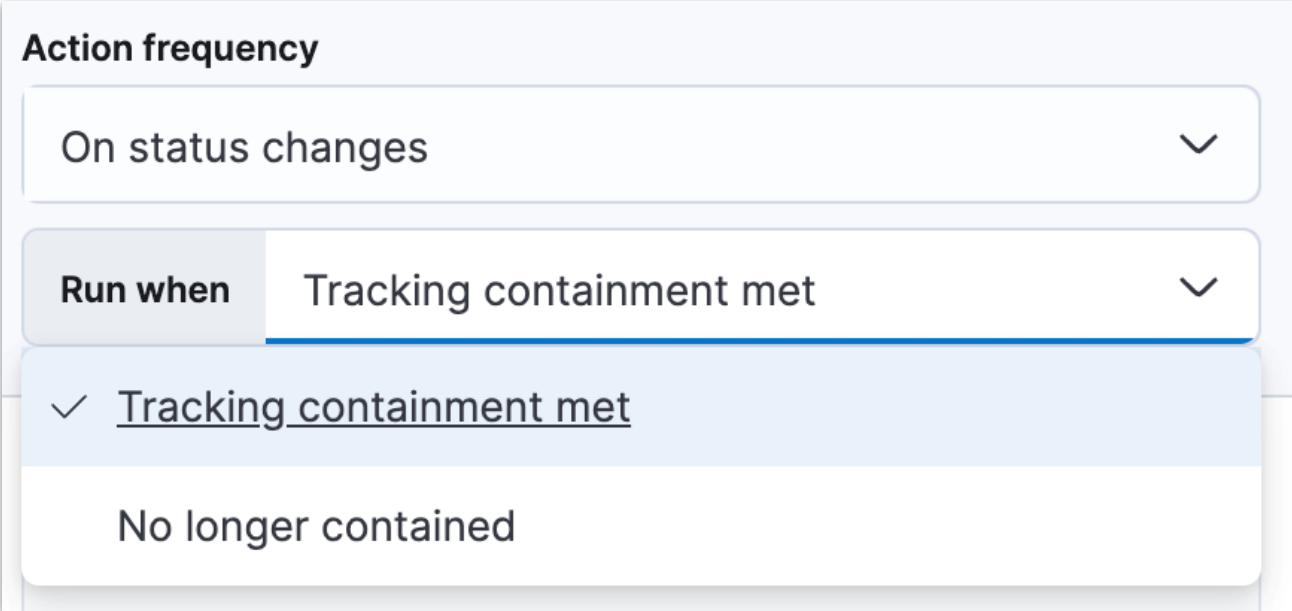
On status changes

Run when

Tracking containment met

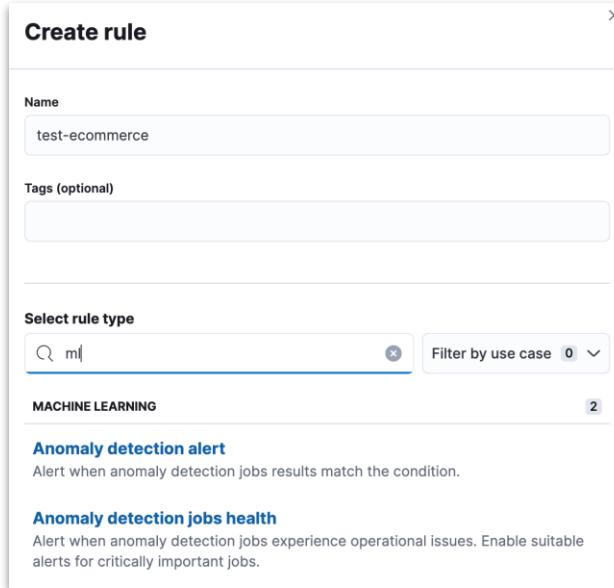
✓ Tracking containment met

No longer contained



# Alerting in ML

- Kibana alerting features include support for machine learning rules
- The following machine learning rules are available



# Creating anomaly detection alert

- Create alert rules from any anomaly detection job

The screenshot shows the Elasticsearch Machine Learning interface. The left sidebar has a 'Machine Learning' icon and sections for Overview, Notifications (4), Memory Usage, Anomaly Detection (with 'Jobs' highlighted by a red box), Anomaly Explorer, Single Metric Viewer, and Settings. The main area is titled 'Anomaly Detection Jobs' and displays two jobs:

ID	Description	Processed rec...	Mem...	Job state	Datafeed s...	Latest tir...
kibana-logs-ui-default-default-log-entry-categories-count	Logs UI: Detects anomalies in count of log entries by category	2,540	ok	opened	started	2023-0
kibana-logs-ui-default-default-log-entry-rate	Logs UI: Detects anomalies in the log entry ingestion rate	2,540	ok	opened	started	2023-0

A context menu is open over the first job, with the 'Create alert rule' option highlighted by a red box. Other options in the menu include Stop datafeed, Clone job, View datafeed counts, Edit job, and Delete job.

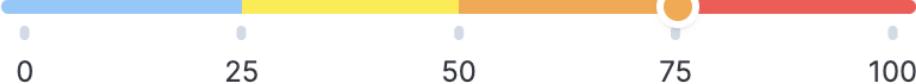
# Creating anomaly detection alert

- Set general rule details
- Select result type and severity level

**Result type**

<b>Bucket</b> How unusual was the job within the bucket of time?  ✓ Selected	<b>Record</b> What individual anomalies are present in a time range?  Select	<b>Influencer</b> What are the most unusual entities in a time range?  Select
---	---	--

**Severity** 75



0 25 50 75 100

# Summary: Creating in-app alerts

Module 8 Lesson 2

# Summary

- You can create alerts from various Kibana apps such as Discover, Maps, Machine Learning, and more...
- Using Tracking containment you can, for example, track the location of an IoT device and monitor a package or vehicle in transit
- You can create a rule to check an anomaly detection job every fifteen minutes for critical anomalies and to notify you in an email

# Quiz

- 1. True or False:** When creating a rule from Discover, the **Create rule** form is pre-filled with the query present in the query bar.
- 2. True or False:** To create a tracking containment rule you only need an index or data view for tracking entities.
3. What three result types can you select when creating an anomaly detection alert?
  - a. Bucket
  - b. Record
  - c. Severity
  - d. Influencer

# Creating in-app alerts

Lab 8.2

# Managing alerts

Module 8 Lesson 3

# Central view

- The **Stack Management > Rules** UI provides a cross-app view of alerting
- It's a central place to
  - Create and edit rules
  - Manage rules
  - Drill-down to rule details
  - Configure settings that apply to all rules in the space

The screenshot shows the 'Rules' section of the Stack Management UI. On the left, there's a sidebar with 'Management' (Ingest Pipelines, Logstash Pipelines), 'Data' (Index Management, Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Cross-Cluster Replication, Remote Clusters, Migrate), and 'Alerts and Insights' (Cases, Connectors, Reporting, Machine Learning, Watcher, Maintenance Windows). The main area is titled 'Rules' with the sub-header 'Detect conditions using rules.' It shows a summary: Succeeded: 1, Failed: 0, Warning: 0. There is 1 rule listed:

Name	Last run	Notify	Int...	Duration	P50	Success ratio	Last response	State
Kibana site - high egr Index threshold	Aug 1, 2023 15:03:32pm a few seconds ago	1	1 hr	00:01	00:01	100%	Succeeded	Enabled

At the bottom, there are buttons for 'Create rule', 'Documentation', 'Settings', and 'Refresh'.

# Managing a rule

- The rule listing enables you to quickly disable, enable and delete individual rules

The screenshot shows the Elasticsearch Stack Management interface, specifically the 'Rules' section. On the left, there's a navigation sidebar with 'Management', 'Ingest', 'Data', 'Alerts and Insights' sections, and 'Rules' under 'Alerts and Insights' is selected. The main area is titled 'Rules' with the sub-instruction 'Detect conditions using rules.' Below this are two tabs: 'Rules' (selected) and 'Logs'. A search bar and several filter dropdowns (Rule state, Type, Action type, Last response, Tags) are available. The main table lists one rule:

Name	Last run	Notify	Int...	Duration	P50	Success rati...	Last response	State
Kibana site - high ege	Aug 2, 2023 Index threshold	15:03:36pm 5 minutes ago	1 hr	00:00	00:00	100%	Succeeded	Enabled

A modal dialog is open over the table, showing a dropdown menu with 'Enabled' (marked with a checkmark) and 'Disabled' options. The 'Enabled' option is highlighted with a pink rectangle. At the bottom of the page, there's a footer with 'Rows per page: 10' and copyright information: '© Copyright Elasticsearch BV 2015-2024 Copying, publishing and/or distributing without written permission is strictly prohibited'.

# Drill-down to rule details

- Select one specific rule from the list to check its details
- For example, you might want to check the status of the rule

Kibana site - high egress

Type Index threshold API key owner training

Rule is Enabled ▾  
24 executions in the last 24 hr

Last response 16 minutes ago  
• Succeeded

Notify when alerts generated

Definition

Rule type Index threshold Actions Demo emails  
Description Alert when an aggregated query meets the threshold.  
Runs every 1 hr  
Conditions 0 conditions

Alerts History

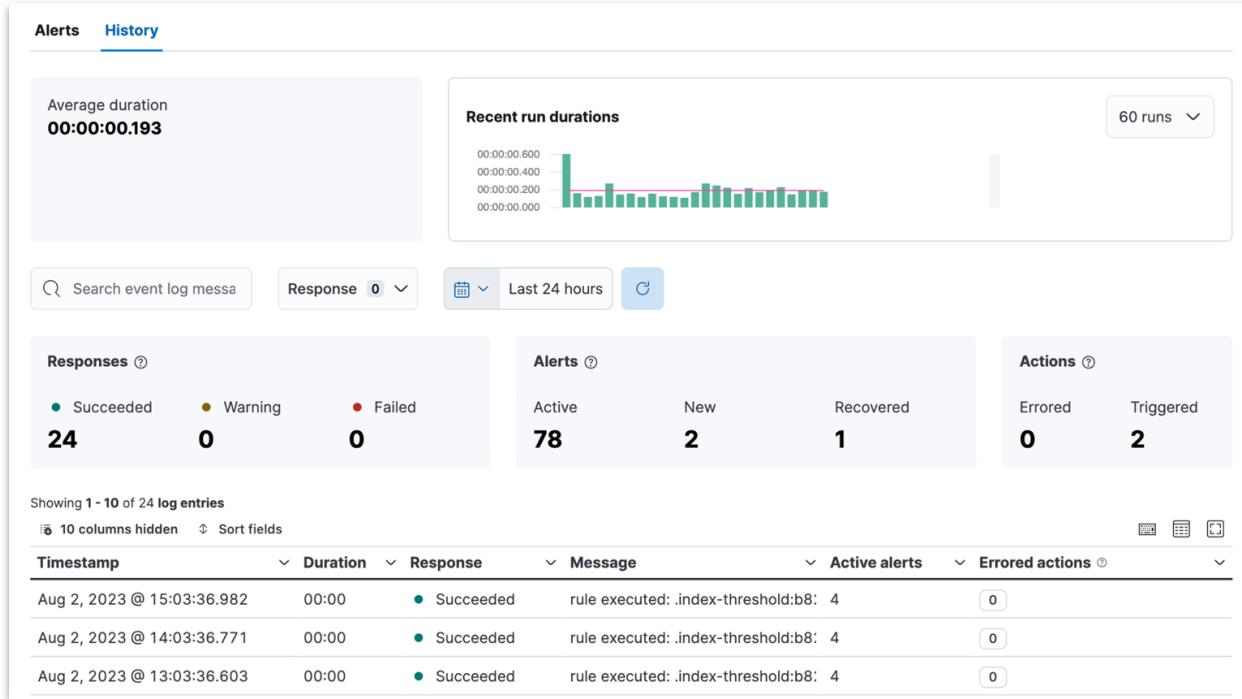
Alert	Status	Start	Duration	Maintenance windows	Mute
artifacts.elastic.co	Active	1 Aug 2023 @ 15:03:33	00:15:37	<input type="checkbox"/>	<input type="checkbox"/>
cdn.elastic-elastic-elastic.org	Active	1 Aug 2023 @ 15:03:33	00:15:37	<input type="checkbox"/>	<input type="checkbox"/>
elastic-elastic-elastic.org	Active	2 Aug 2023 @ 11:03:36	04:15:34	<input type="checkbox"/>	<input type="checkbox"/>
www.elastic.co	Active	1 Aug 2023 @ 15:03:33	00:15:37	<input type="checkbox"/>	<input type="checkbox"/>

# Which status a rule can have?

- **Active:** The conditions for the rule have been met, and the associated actions should be invoked
- **OK:** The conditions for the rule have not been met, and the associated actions are not invoked
- **Error:** An error was encountered by the rule
- **Pending:** The rule has not yet run. The rule was either just created, or enabled after being disabled
- **Unknown:** A problem occurred when calculating the status. Most likely, something went wrong with the alerting code

# Rule history

- You can also check the history of the rule



# Snooze a rule

- Accessing one specific rule also allows you to snooze it
- When you snooze a rule, the rule checks continue to run on a schedule, but the alert will not trigger any actions
- You can either snooze for a specified period of time or indefinitely

The image contains two side-by-side screenshots of the Elasticsearch interface.

**Left Screenshot:** Shows a rule configuration page. The top section displays "Rule is Enabled" and "24 executions in the last 24 hr". Below this, the "Last response" section shows "2 minutes ago" and "Succeeded". At the bottom, there is a "Notify when alerts generated" button with a bell icon.

**Right Screenshot:** Shows the "Snooze notifications" section of the rule configuration. It includes a summary: "24 executions in the last 24 hr". The main area has a heading "Snooze notifications" with the sub-instruction "Silence actions immediately or schedule downtimes." Below this, a "Last response" section shows "3 days". A "Commonly used" section lists "1 hour", "3 hours", "8 hours", and "1 day". A "Snooze indefinitely" section is present. At the bottom is a large blue "Add schedule" button.

# Maintenance windows

- You can schedule single or recurring maintenance windows to temporarily reduce rule notifications

The screenshot shows the Elasticsearch Stack Management interface with the 'Maintenance Windows' tab selected. The left sidebar includes sections for Management (Ingest, Data, Alerts and Insights), with 'Maintenance Windows' highlighted with a pink rectangle. The main area displays a table of maintenance windows:

Name	Status	Start time	End time	Actions
Monthly maintenance window	Upcoming	07/14/23 02:00 PM	07/14/23 03:00 PM	...

Below the table are search and status filters, and pagination controls.

# Troubleshooting

- Test the connectors and rules
- Check the Kibana logs
- Use Task Manager diagnostics
- Use REST APIs
- Look for error banners
- Refer to the documentation

<https://www.elastic.co/guide/en/kibana/current/alerting-troubleshooting.html>

# Limitations

- Known limitations until Kibana version 8.8
- Alerts are not visible in **Stack Management > Rules**
  - when you create a rule in Observability or Elastic Security apps
- You can view them only in the Kibana app where you created the rule

# Summary: Managing alerts

Module 8 Lesson 3

# Summary

- The Rules UI allows you to create, edit, disable or delete one or more rules
- You can click a rule name to access the details page for the rule where you can see currently active alerts and history
- Accessing Kibana logs, using the Task Manager and checking error banners are different ways to troubleshoot rules

# Quiz

- What are the 5 status rules?
- **True or False:** You can delete multiple rules at once.
- **True or False:** You cannot indefinitely snooze a rule.

# Managing alerts

Lab 8.3



# Conclusion

# Resources

- <https://www.elastic.co/learn>
  - <https://www.elastic.co/training>
  - <https://www.elastic.co/community>
  - <https://www.elastic.co/docs>
- <https://discuss.elastic.co>
  - <https://ela.st/training-forum>
- <https://ela.st/slack>

# Elastic Support Hub

- <https://support.elastic.co/home>
  - access a wealth of technical resources
  - maximize your experience using Elastic solutions

The screenshot shows the Elastic Support Hub homepage. At the top left is the "Elastic Support" logo. On the right is a blue "Open case" button. Below the header, there's a navigation bar with tabs: "Recommended For You" (highlighted), "Newest Articles", and "Recently Viewed".  
  
The main content area displays four recommended articles:

- How to fix a broken Kibana Monitoring UI for an ESS cluster after upgrading to v8** (Last updated 7 months ago)
- Where is kibana audit log stored when it is configured in Elastic Cloud** (Last updated 5 months ago)
- Enabling Metrics collection on Elasticsearch Service may create a lot of data** (Last updated 4 months ago)
- How to schedule hit Cluster Reroute API with retry.failed to retry failed shards** (Last updated 4 months ago)

  
To the right of the articles is a promotional box for "Start your Elastic Cloud trial". It features the Elastic logo and a call-to-action button "Create deployment".  
  
Below the trial box is another section titled "Talk to Elastic Support" with a "Get set up >" button.

# Elastic Certification

## Validate Skills

Apply practical knowledge with performance-based testing

## Boost Productivity

Overcome obstacles with confidence and ease as you move from dev to production

## Open New Doors

Enhance professional visibility and expand opportunities

## Join the Community

Become part of an exclusive network of over 1,000 certified professionals in nearly 70 countries



Elasticsearch  
Engineer

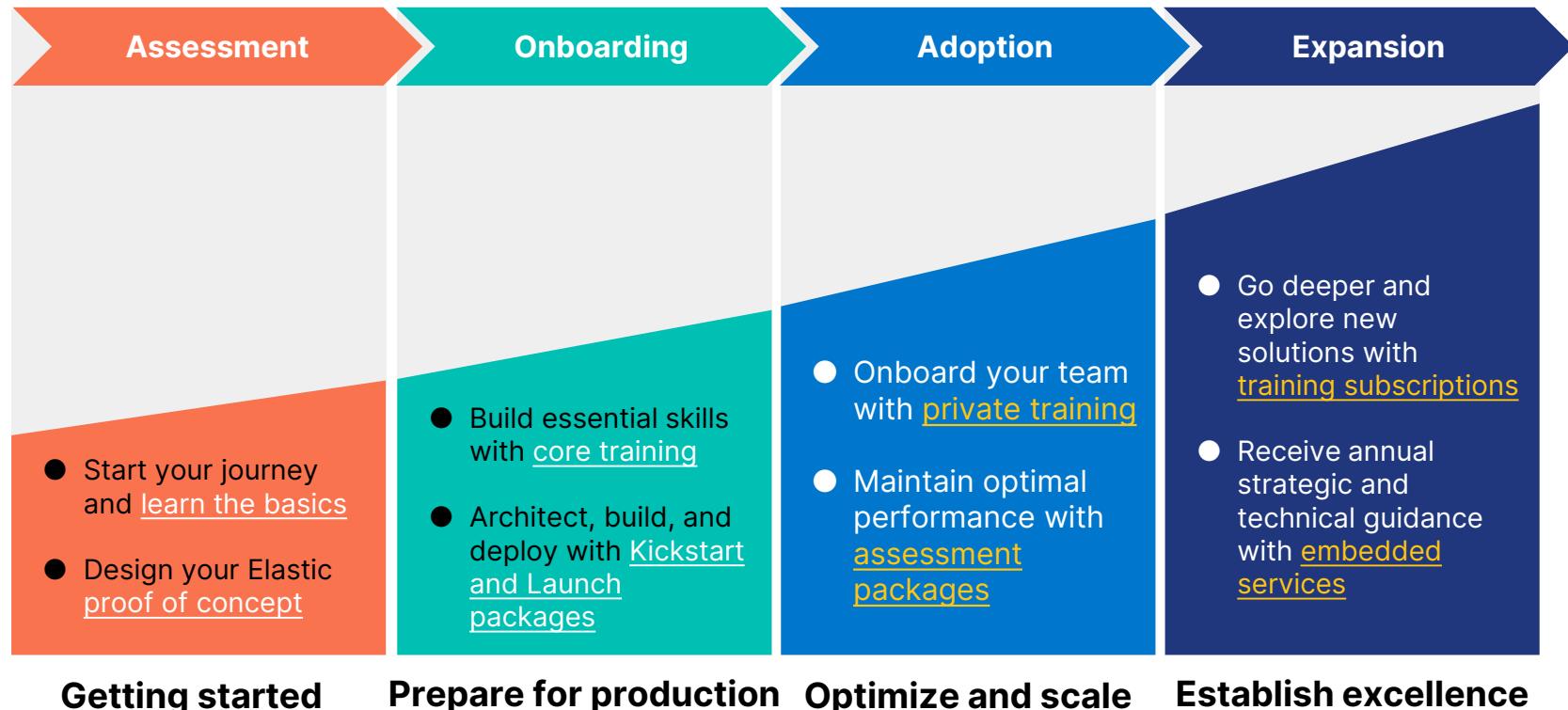


Data Analyst



Observability  
Engineer

# Elastic Enablement Journey



The background features abstract graphic elements: a yellow-to-orange gradient bar at the top right, a blue square with a circular pattern, a large dark blue circle with a pink speckled sphere, and a vertical bar composed of orange, black, and teal segments.

**Thank You**  
Please complete  
the survey

# Quiz Answers

## 1.1 Introduction to Kibana

1. True
2. True
3. False. Data is stored in Elasticsearch. Kibana is the user interface for Elasticsearch

## 1.2 Hello, Dashboard

1. True
2. Lens (or Maps for geo data)
3. True. You can copy visualizations from one dashboard to another

## 1.3 Your Space

1. True
2. Create a different space for each user
3. Go to Saved Objects and copy the dashboard and all associated assets to the other space

## 2.1 Discover and Data Visualizer

1. Index pattern and time filter
2. False. Data Visualizer will show you a summary of every field. Use the Discover tool to examine specific documents
3. Geopoint

## 2.2 KQL and filters

1. False. Kibana can handle many filters at the same time and you can choose to enable or disable any or all of them
2. Filter actions are: (1) Pin across all apps (2) Edit filter (3) Include/Exclude results (4) Enable/Temporarily disable (5) Delete
3. The boolean operators in KQL are: **and or not**

## 2.3 Field focus

1. False. When you try to visualize geopoint data, it opens up the Maps editor
2. Layer pane
3. False. Use the Chart type drop down menu to select the visualization style you like

## 3.1 Create visualizations

1. False. The underlying operation in Elasticsearch is the same between a pie chart and a bar graph. Data is grouped by some criteria (like values of a particular field) then some metric is computed for each grouping (like the number of documents in the group). This is called an Elasticsearch aggregation
2. Bar or area percentage views will display how one group compares proportionally to another group
3. In the layer pane, change **Number of views**

## 3.2 Adjust visualizations

1. True. For example, changing the axes of overlapping charts can clarify details of each of the separate charts while also displaying how they line up
2. Use time shift to see data from a previous week right next to your current week
3. False. Go to the dashboard options to disable panel titles

## 3.3 Create maps

1. True
2. At least two
3. Layer actions are: (1) Fit to data (2) Show/Hide layer (3) Edit layer settings (4) Clone layer (5) Remove layer

## 4.1 Text and metrics

1. For multiple metrics arranged in a grid, use the Break down field
2. Create links to other dashboards
3. Text uses a GitHub-flavored markdown syntax

## 4.2 Tables

1. True
2. False. Conditional coloring can be set for values in a table, not just a column
3. True

## 4.3 Interactive dashboards

1. False. Click directly on the visualizations to create filters
2. There are many ways to create filters: Clicking Add filter in the top left, clicking a value in a visualization, and selecting a value in a Control
3. Drillsdowns can send you to another dashboard with selected filters enabled or open an URL using parameters from your filters

## 5.1 Sharing a dashboard

1. False. Reports can also be generated using Discover or Canvas
2. False. Links will always get the latest updated data, but may not reflect changes to the dashboard itself
3. If you want to keep a static record of a point in time of your data

## 5.2 Sharing with users

1. Roles
2. Anonymous authentication will provide access to all of Kibana, so restrict what the privilege of the anonymous user
3. A given role can be assigned to a specific space with only limited features enabled

## 5.3 Canvas

1. True
2. Elasticsearch SQL, Elasticsearch documents, Timelion, Demo data
3. Starting a new workpad, which can also use a template

## 6.1 Introduction to Elastic Machine Learning

1. False. Set up rules to be alerted whenever an anomaly is detected
2. Calendar events or model snapshots
3. Calendar events can be used to exclude future events; model snapshots can be used to rerun the job to forget past events

## 6.2 Analyzing anomaly detection results

1. True
2. False. The results of machine learning jobs are stored in Elasticsearch. You can explore that data in Discover, or visualize it on a dashboard
3. False. You can annotate your job results in the Single Metric Viewer

## 6.3 Data frame analytics

1. True
2. False. Transforms creates a new index with the transformed data
3. Pivot and latest

## 6.4 AIOps Labs

1. Explain log rate spikes/Log pattern analysis/Change point detection
2. Change point detection
3. No, it works best on unstructured data. Using it on the country\_name field will simply lead to the same result in the “top values” section of the discover app

## 7.1 Formulas

1. True. Use the “KQL” or “lucene” argument
2. True. Use the “shift” argument
3. False. This formula finds the percentage of visitors to a webpage that received a not found error

## 7.2 Runtime fields

1. False. Runtime fields are scripted in Painless
2. Use **emit** to return values of a runtime field
3. False. Runtime fields are great to create values on the fly, but if you want to access those values regularly, it is more efficient to index a new field with those values

## 7.3 Vega

1. True
2. True
3. False. Vega visualizations can be made to react to dashboard filters, including the time filter

## 8.1 Rules and Connectors

1. The three building blocks of rules are: Conditions, Schedule, and Actions
2. False. The four rules can use the same connector
3. False. Scheduled checks for Watcher are run on Elasticsearch instead of Kibana

## 8.2 Creating in-app alerts

1. True
2. False. Tracking containment rule requirements include: tracks index or data view and boundaries index or data view
3. The three result types you can select when creating an anomaly detection alert are: Bucket, Record, and Influencer

## 8.3 Managing alerts

1. The 5 status rules are: Active, Ok, Error, Pending, and Unknown
2. True
3. False. You can snooze a rule indefinitely (or for a specified period of time)