

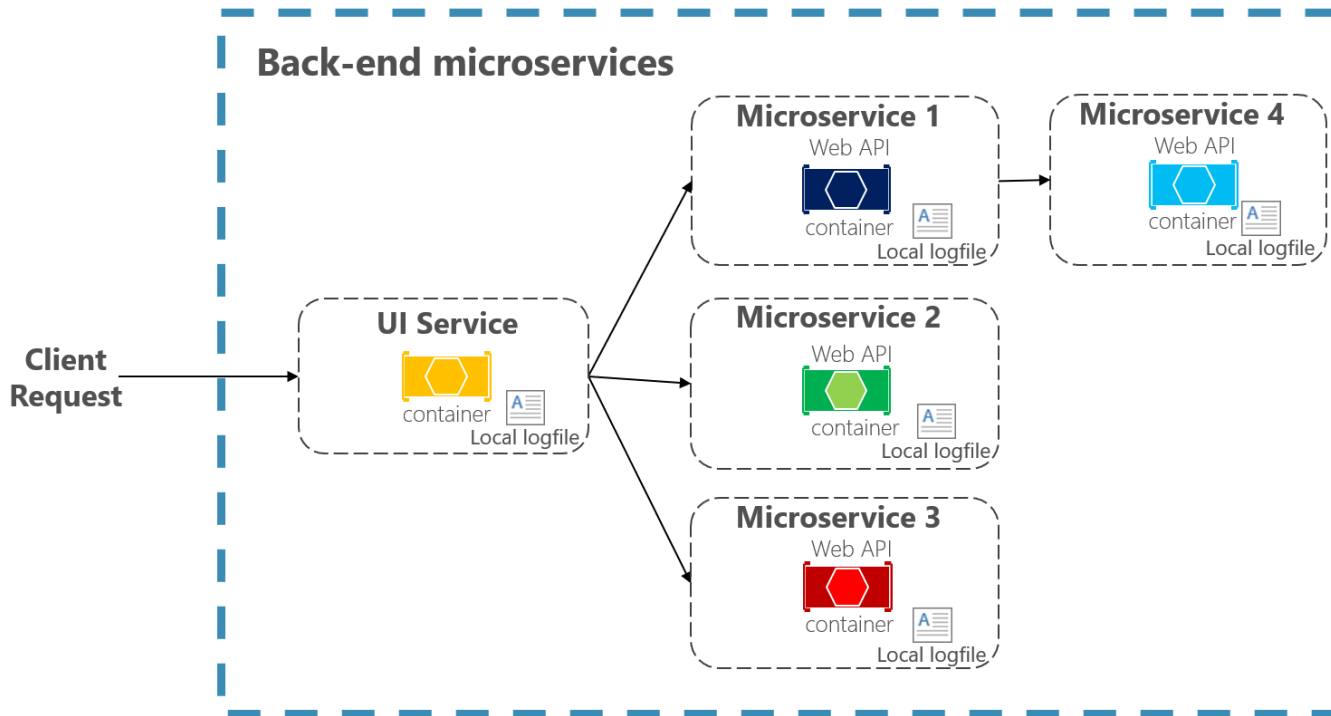


پیاده سازی لاگ متمرکز برای  
میکرو سرویس ها  
به کمک **ELK**

مدرس: مهندس ارومند



# چه خواهیم آموخت؟



۱. Log و کاربرد آن

۲. لاگ ساختار یافته

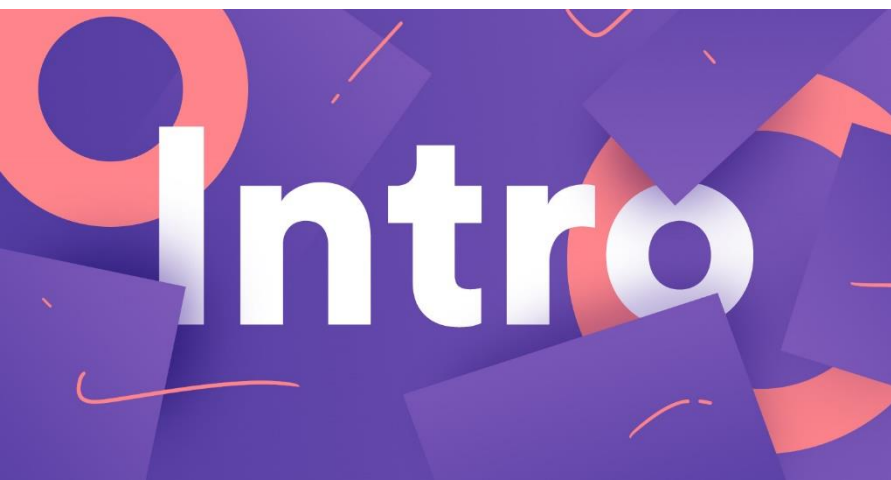
۳. لاگ در میکروسرویس‌ها

۴. واکنشی اطلاعات از لاگ

۵. مصورسازی Logها در Kibana

# مقدمه

۱. پر کاربرد و مغفول واقع شده
۲. خطاهایی که فقط در محیط عملیاتی رخ می‌دهد
۳. فرایند ثبت وقایع و فعالیت‌ها را لاگ کردن می‌نامیم
۴. امکان ثبت در console, file, Evet log و ...



# انواع اصلی Log Message ها

۱. Information مثلا لاگین کردن، ثبت خرید و ...
۲. Error خطا در عملیات سیستم، مثل Exception
۳. Warning وقایع سیستم که ممکن است به Error برسد





# استفاده موثر از Log

۱. ابزاری برای تشخیص خطا
۲. نگهداری خطا کاری بسیار مهم
۳. روال منجر به خطا کمک کننده
۴. لاگ برای تحلیل و بررسی
۵. لاگ برای رسیدن به خطا

# تشخیص مشکل با Log

۱. مقدار زیادی Log پیش فرض

۲. پوشش اکثر مشکلات

۳. خطای اختصاصی وضوح بیشتر

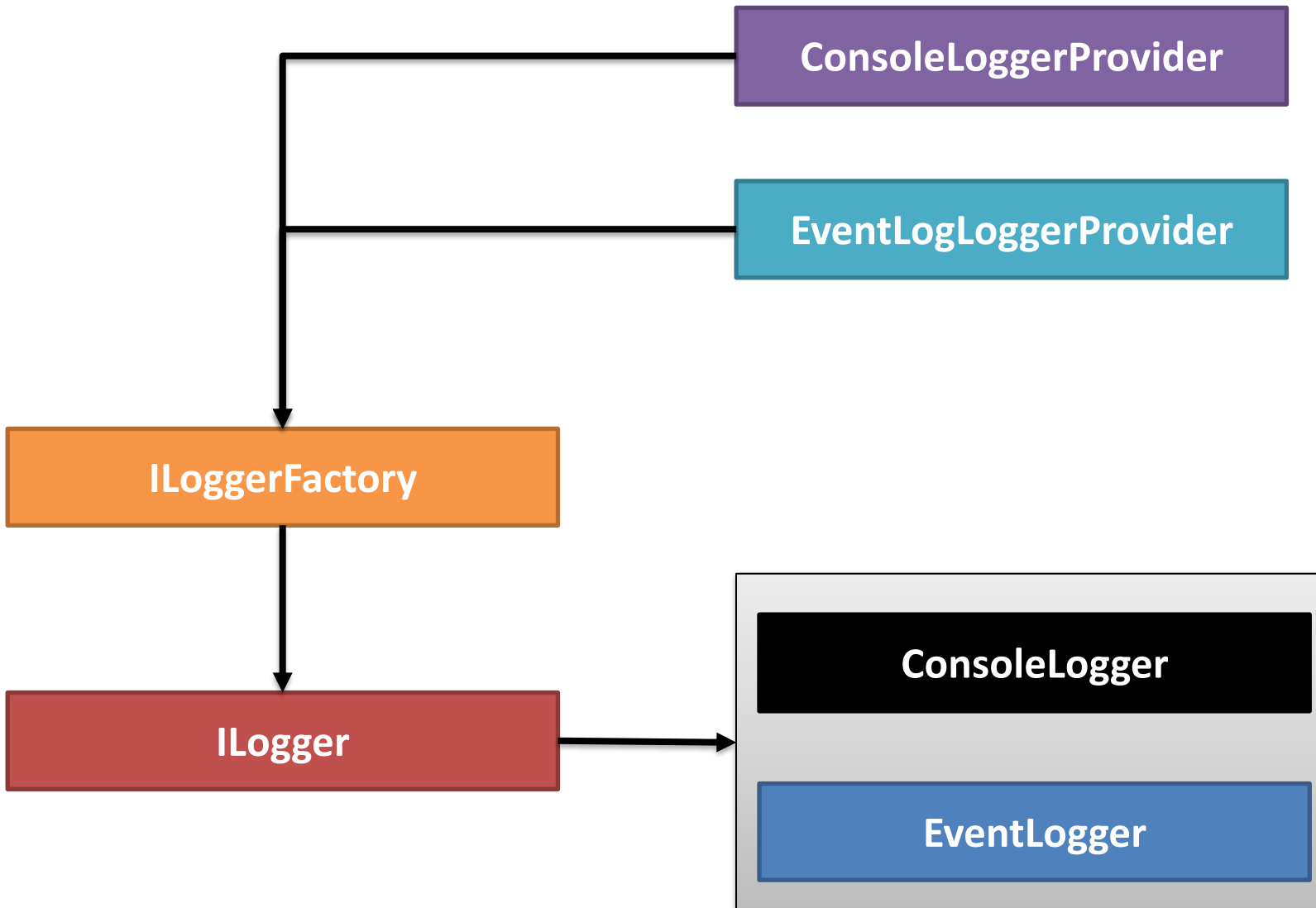


# زیر ساخت موجود

۱. ILogger

۲. ILoggerProvider

۳. ILoggerFactory



# استفاده از زیرساخت برای Log

۱. چگونه یک Log Message ایجاد کنیم؟
۲. چگونه افزودن Log به کمک ILogger
۳. ویژگی‌های مهم Log Message
۴. افزودن مقدار به پیام با {Placeholder}



# بررسی ساختار Log

۱. Log Level

۲. Event Category

۳. Message

۴. Parameters

۵. Exceptions

۶. EventId

```
C# G:\Src\Vs\LogTest\LogTest\bin\Debug\net5.0\LogTest.exe
```

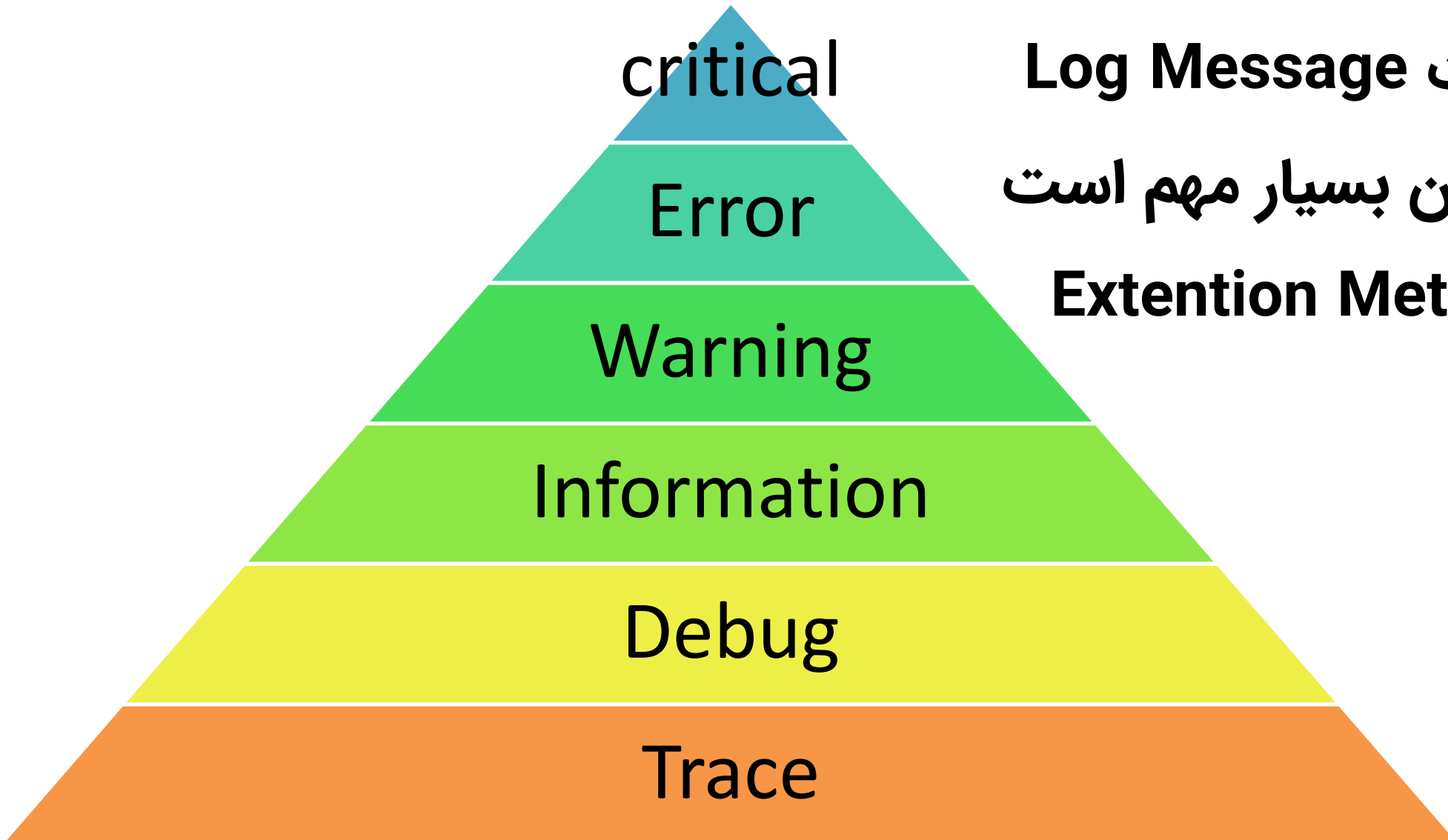
```
Now listening on: http://localhost:5000
```

```
info: Microsoft.Hosting.Lifetime[0]  
Application started. Press Ctrl+C to shut down.
```

```
info: Microsoft.Hosting.Lifetime[0]  
Hosting environment: Development
```

```
info: Microsoft.Hosting.Lifetime[0]  
Content root path: G:\Src\Vs\LogTest\LogTest
```

# Log Level



۱. تعیین اهمیت Log Message
۲. برای فیلترکردن بسیار مهم است
۳. تنظیم با Extention Method

# Log Category

۱. روشی برای گروه بندی

۲. تنظیم هنگام نمونه سازی از ILogger

۳. مقدار متنی است



# ساختار دهی به پیام

۱. پیام شامل هر رشته‌ای می‌باشد

۲. امکان ارسال Placeholder

۳. استفاده از کلیدها در Structured Log

۴. عدم پشتیبانی توسط همه Providerها



# تعیین محل نگهداری Log

۱. فقط نمایش در Console کافی نیست
۲. عدم کاربرد در محیط عملیاتی
۳. تعیین به کمک Log Provider ها

**Console Log Provider**

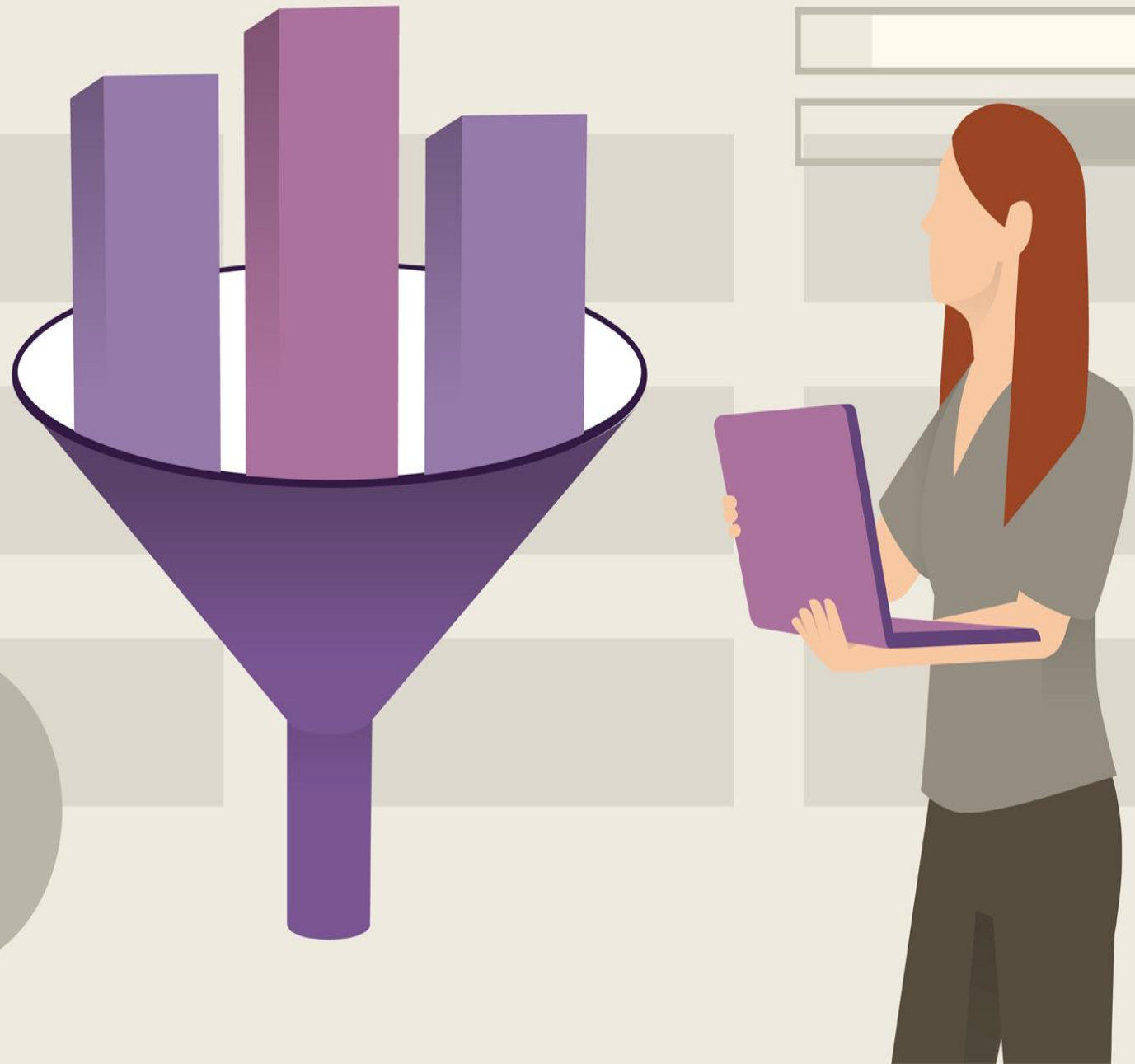
**Debug Log Provider**

**EventSource Log Provider**

**EventLog Log Provider**

# کنترل تعداد Logها

۱. هدف کاهش حجم Log
۲. مدیریت بر اساس سطح Log
۳. مدیریت بر اساس Provider
۴. مدیریت به کمک Category



# آشنایی با Structured Log

۱. اطلاعات زیادی در قالب متن
۲. نیاز به تحلیل داده‌های متنی
۳. نگهداری داده‌ها و ساختار
۴. قابلیت استفاده ساده‌تر
۵. تحلیل پذیری بالا
۶. به طور معمول نگهداری Json



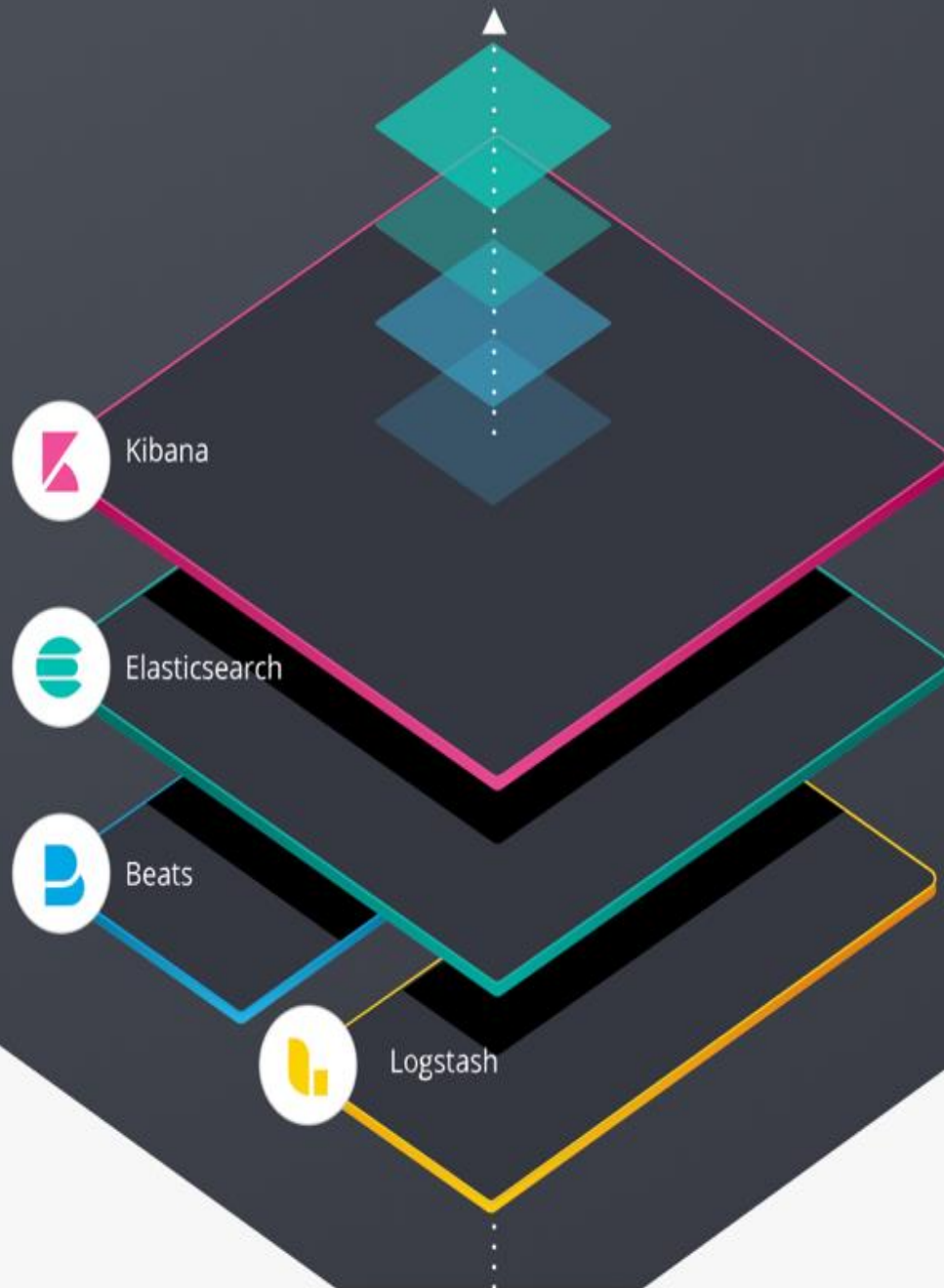
**SCHEMA**

# ابزارهای مناسب

۱. ELK

۲. Splunk

۳. Seq





# آشنایی با Scope

۱. نیاز به اشتراک داده در Log
۲. تعریف Scope در هر قالبی
۳. همه Log ها Scope را خواهند داشت



# آشنایی با Serilog

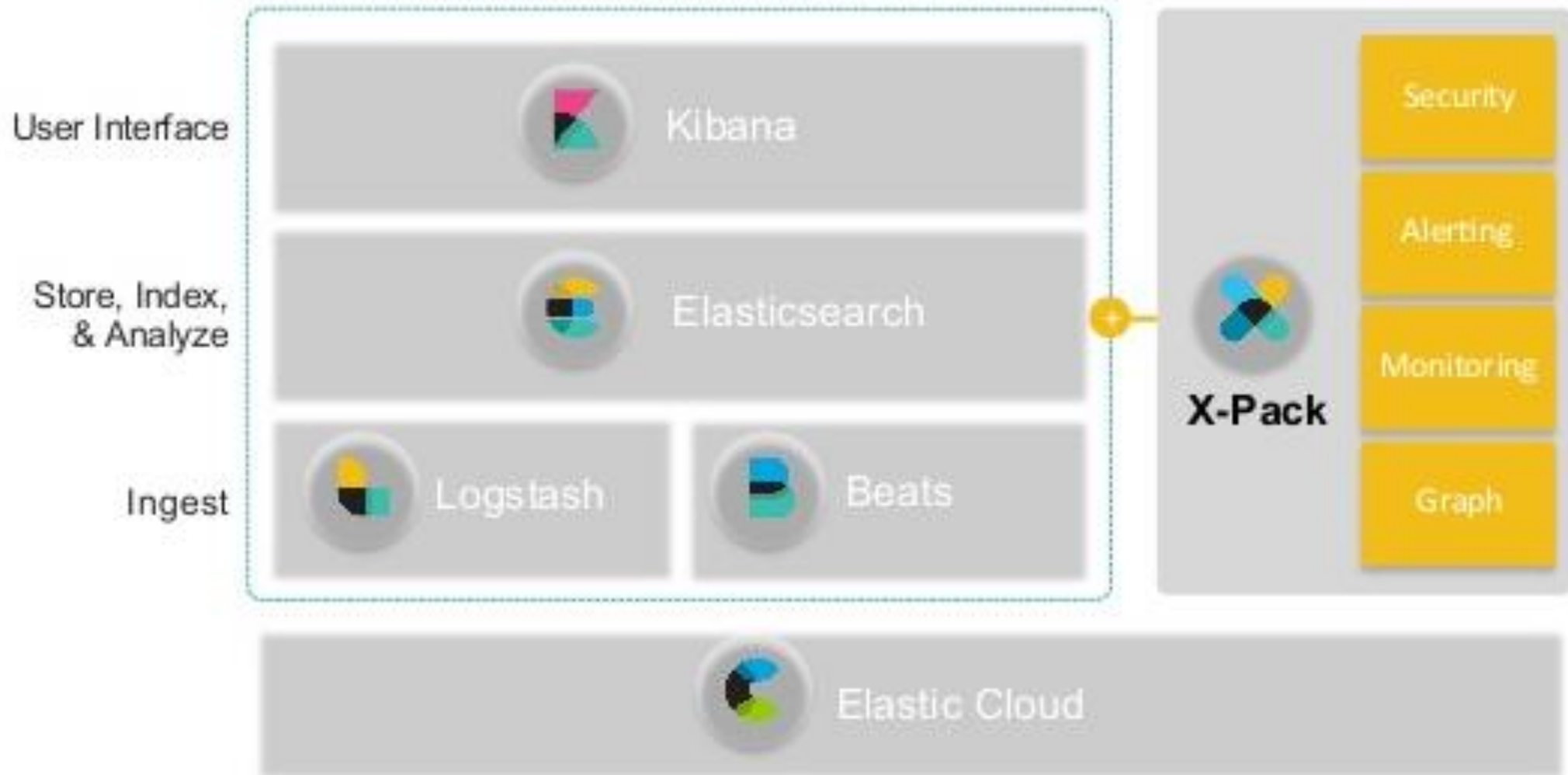
۱. کتابخانه‌های Structured Log
۲. محل‌های مختلف با Sinkها
۳. امکان غنی سازی با Enricher



# Log در میکروسرویس‌ها

۱. چندین سرویس مختلف
۲. از هر سرویس چندین نمونه اجرایی
۳. تکنولوژی‌های متفاوت برای توسعه
۴. نیاز به تجمیع Logها در یک محل
۵. نیاز به شناسایی Logهای مرتبط
۶. نیاز به دانستن وقایع زیرساختی

# آشنایی با ELK



# Elasticsearch

۱. قلب تپنده سیستم
۲. ذخیره داده‌ها و قابلیت جستجو و تحلیل
۳. قابلیت استفاده به تنهایی برای جستجو



# elasticsearch

# Logstash

۱. راهکار جریان ورودی داده‌ها
۲. تبدیل و به روزرسانی داده‌ها قبل از ذخیره
۳. مجتمع سازی داده‌های تبدیل یافته
۴. یک ابزار سمت Server
۵. مبتنی بر Plugin



# logstash

# Beats

1. تکمیل کننده Logstash
2. یک ابزار Client side
3. وظیفه ارسال داده برای سرور



beats

# Kibana

۱. ابزار Visualization
۲. توانایی نمایش داده‌های
۳. پنجره ورودی به دنیای Elastic
۴. ارائه ابزارهای مدیریتی و توسعه



# kibana





## X-Pack

1. امنیت
2. مانیتورینگ
3. هشدار
4. گزارش دهی
5. گراف
6. یادگیری ماشین

# x-pack

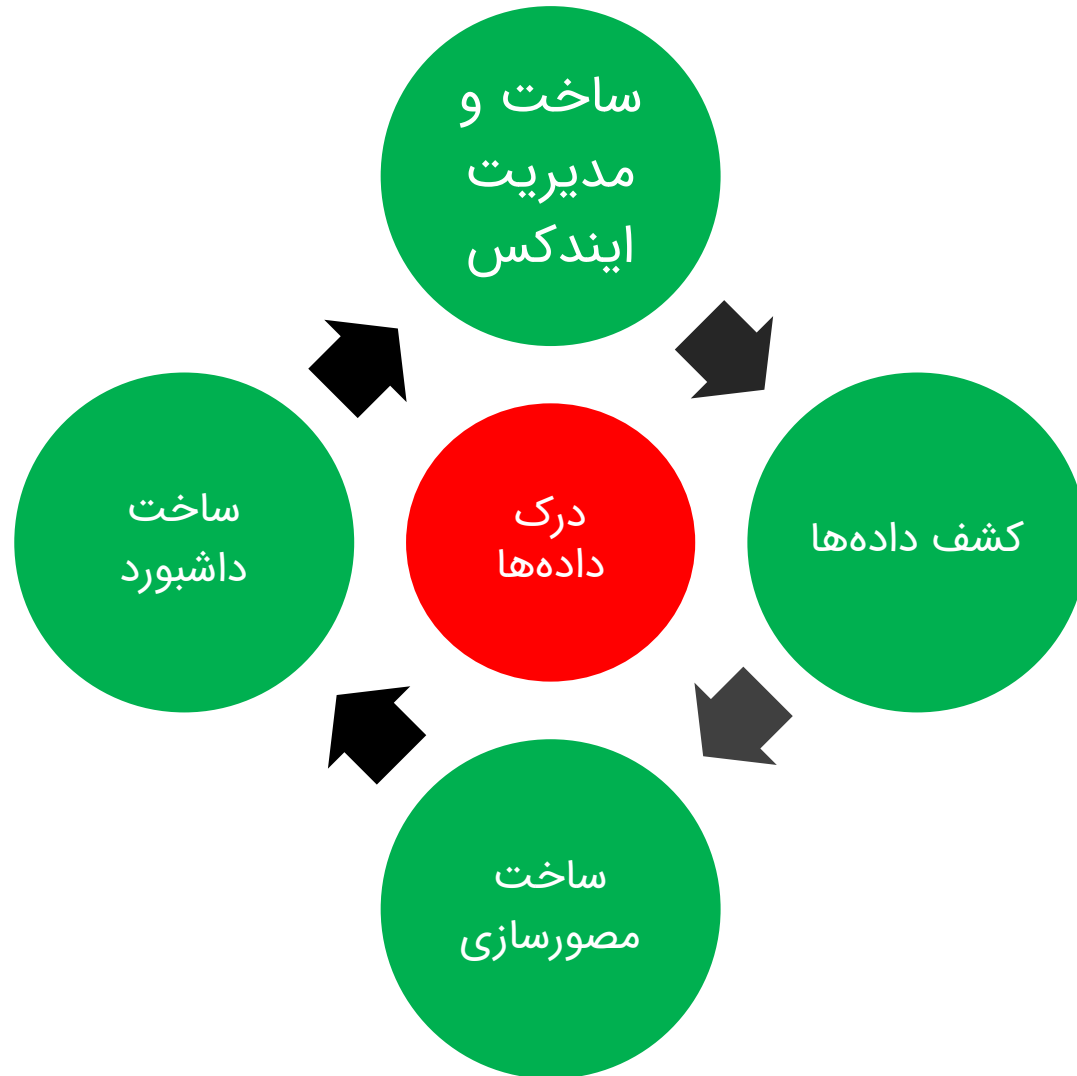
# نگهداری Log ها در Elasticsearch















۱. نصب Sink مربوط به Elasticsearch
۲. انجام تنظیمات مرتبط با Elasticsearch
۳. نصب و راه اندازی Elasticsearch

# آشنایی با Kibana UI

۱. تعامل کاربر
۲. تنظیمات ایندکسها
۳. نمایش دادهها
۴. ساخت داشبورد

# تعاملات کاربران



-  Discover
-  Visualize
-  Dashboard
-  Canvas
-  Maps
-  Machine Learning
-  Metrics
-  Logs
-  APM
-  Uptime
-  SIEM
-  Dev Tools
-  Stack Monitoring
-  Management

# بخش‌های مهم

**Discover .۱**

**Visualize .۲**

**Dashboard .۳**

**Dev Tools .۴**

**Management .۵**

# ایجاد الگوی Index

۱. باید الگوی ایندکس داشته باشیم
۲. تعیین ایندکس‌های شرکت کننده
۳. امکان تعیین چندین ایندکس

## Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Include system indices

### Step 1 of 2: Define index pattern

Index pattern

logstash-\*

You can use a \* as a wildcard in your index pattern.

You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ **Success!** Your index pattern matches **1 index**.

> Next step

# دو نوع معمول Index

۱. Time-series Index

۲. Regular Index

## Step 2 of 2: Configure settings

You've defined **logstash-\*** as your index pattern. Now you can specify some settings before we create it.

Time Filter field name Refresh

The Time Filter will use this field to filter your data by time.  
You can choose not to have a time field, but you will not be able to narrow down your data by a time range.

> Show advanced options

# Discover



۱. کمک به شناخت داده‌ها
۲. جستجو و مشاهده نتیجه
۳. امکان ذخیره کوئری‌های پرکاربرد
۴. نمایش وقایع ۱۵ دقیقه اخیر



# بخش‌های پر کاربرد



**Index Pattern .۱**

**Field List .۲**

**Document Table .۳**

**Query Bar .۴**

# Lucene یا KQL

۱. امکان انتخاب در بخش جستجو

۲. پیش فرض KQL



# جستجوی Lucene

۱. جستجوی متن عادی
۲. جستجوی فیلد خاص
۳. قابلیت استفاده از Logical Operator
۴. قابلیت گروه‌بندی
۵. جستجوی محدوده
۶. wildcard

# DSL Query

۱. اجرا در Query Bar

۲. نمایش تعداد اسناد نتیجه



# KQL Query

۱. Kibana Query Language

۲. ساده سازی کوئری نویسی



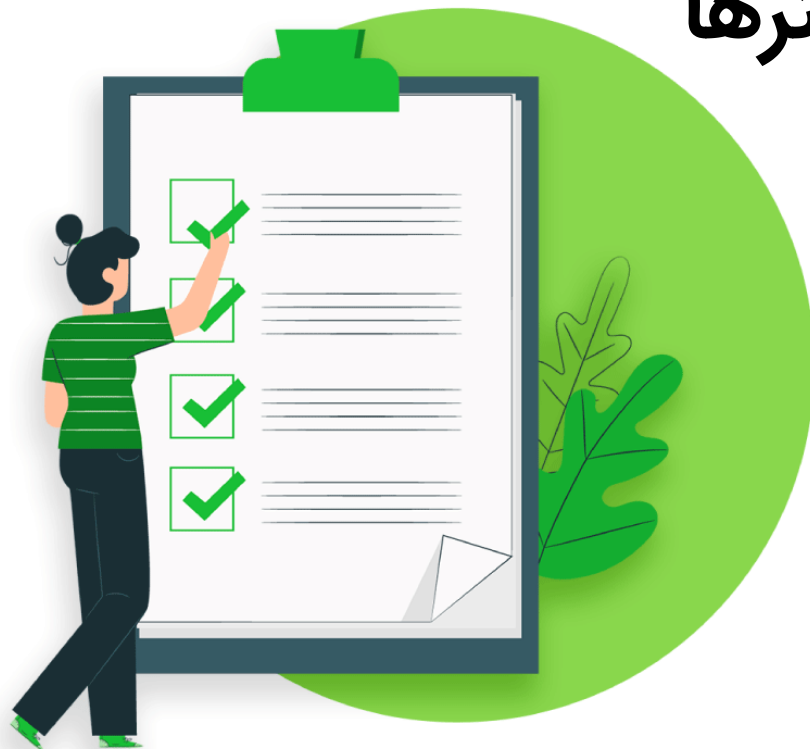
# kibana

# سایر ویژگی‌های کوئری نویسی

۱. امکان ذخیره
۲. اشتراک گذاری کوئری‌ها
۳. بررسی عملکرد کوئری
۴. انتخاب زمان در صورت دارا بودن فیلد زمان

# امکانات داخلی صفحه

۱. نمایش نتیجه به صورت جدول و JSON
۲. ارائه امکان فیلترکردن داده‌ها در جدول
۳. قابلیت ایجاد و مدیریت دستی فیلترها



# ویژگی‌های فیلترها

۱. امکان فعال/غیرفعال
۲. Pin کردن یک فیلتر
۳. تغییر نمایش یا عدم نمایش منتخبین
۴. حذف فیلتر
۵. ویرایش فیلتر
۶. باز و بستن
۷. عملیات دسته جمعی



# visualize

۱. امکان ایجاد خروجی تصویری
۲. ارائه درک بهتر از داده‌ها
۳. بر مبنای Aggregation Query



Create your first visualization

You can create different visualizations, based on your data.

[+ Create new visualization](#)

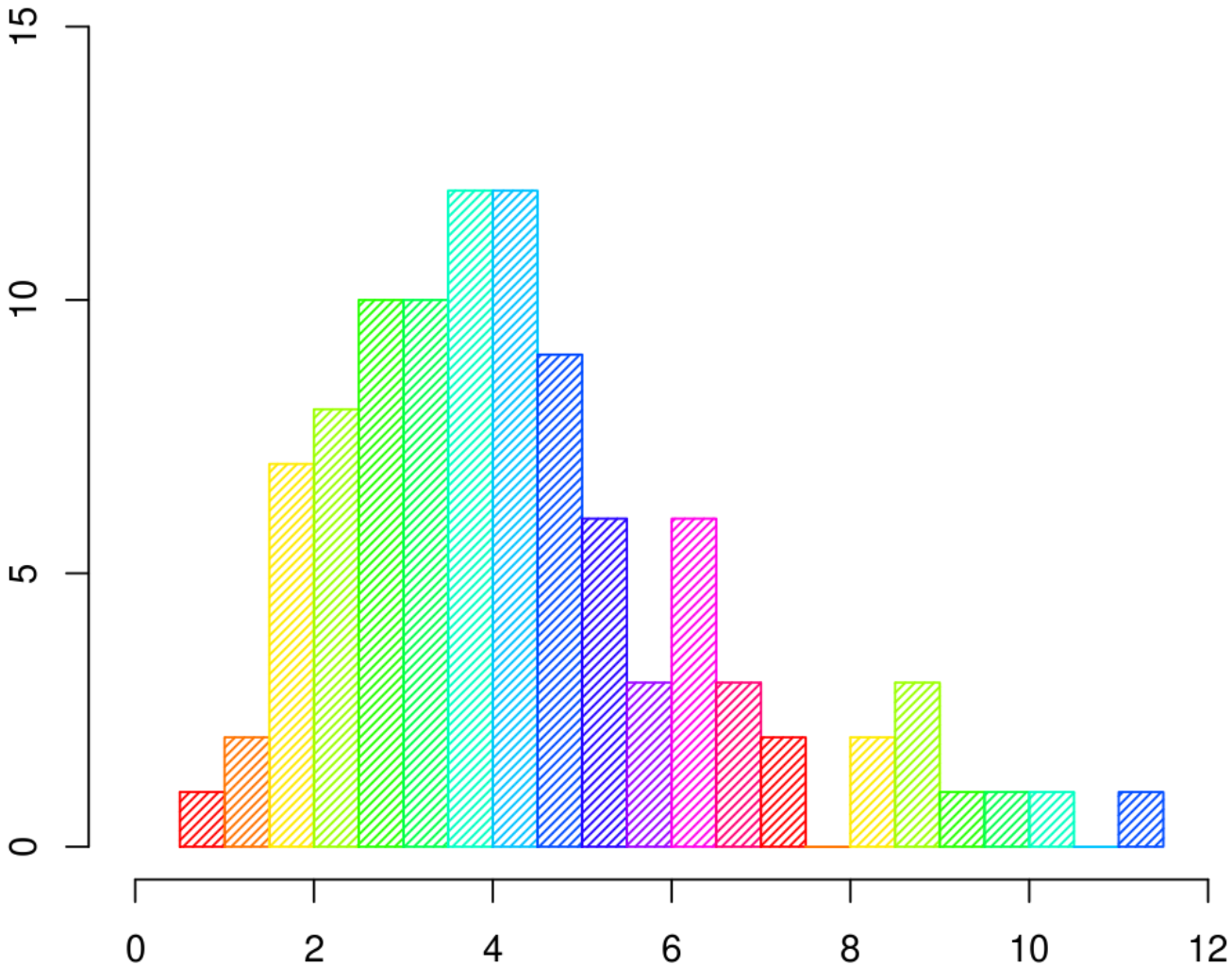
# Kibana Aggregation

**Bucket Aggregation ۱.**

**Metric Aggregation ۲.**



# Bucket Aggregation



**Histogram .۱**

**Date Histogram .۲**

**Range .۳**

**Terms .۴**

**Filters .۵**

**GeoHash Grid .۶**

# Metric Aggregation



- Count .۱**
- Average .۲**
- Sum .۳**
- Median .۴**
- Min/Max .۵**
- Standard Deviation .۶**
- Percentile .۷**
- Percentile Ranks .۸**

# ایجاد Visualization

۱. ایجاد یک Visualization جدید

۲. انتخاب نوع نمایش

۳. انتخاب منبع داده

۴. ساخت Visualization



Create your first visualization

You can create different visualizations, based on your data.

[+ Create new visualization](#)

# اجزای Visualize

۱. Visualization designer

۲. Visualization preview

۳. Label

۴. Query Bar

۵. Toolbar

۶. Filter



# انواع روش‌های نمایش

Line Chart .۱

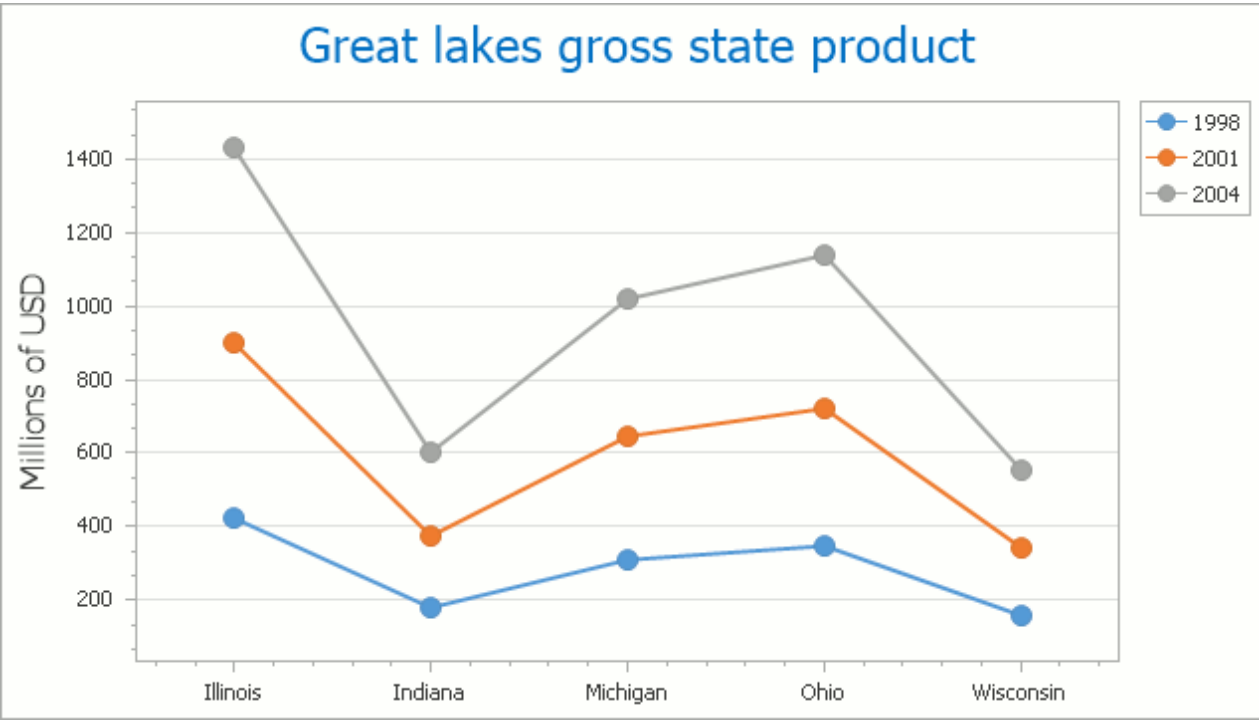
Area Chart .۲

Bar Chart .۳

Data Table .۴

Markdown widgets .۵

Metrics .۶



# انواع روش‌های نمایش

**Goals .1**

**Gauges .۲**

**Pie Chart .۳**

**map .۴**

**Tag Cloud .۵**

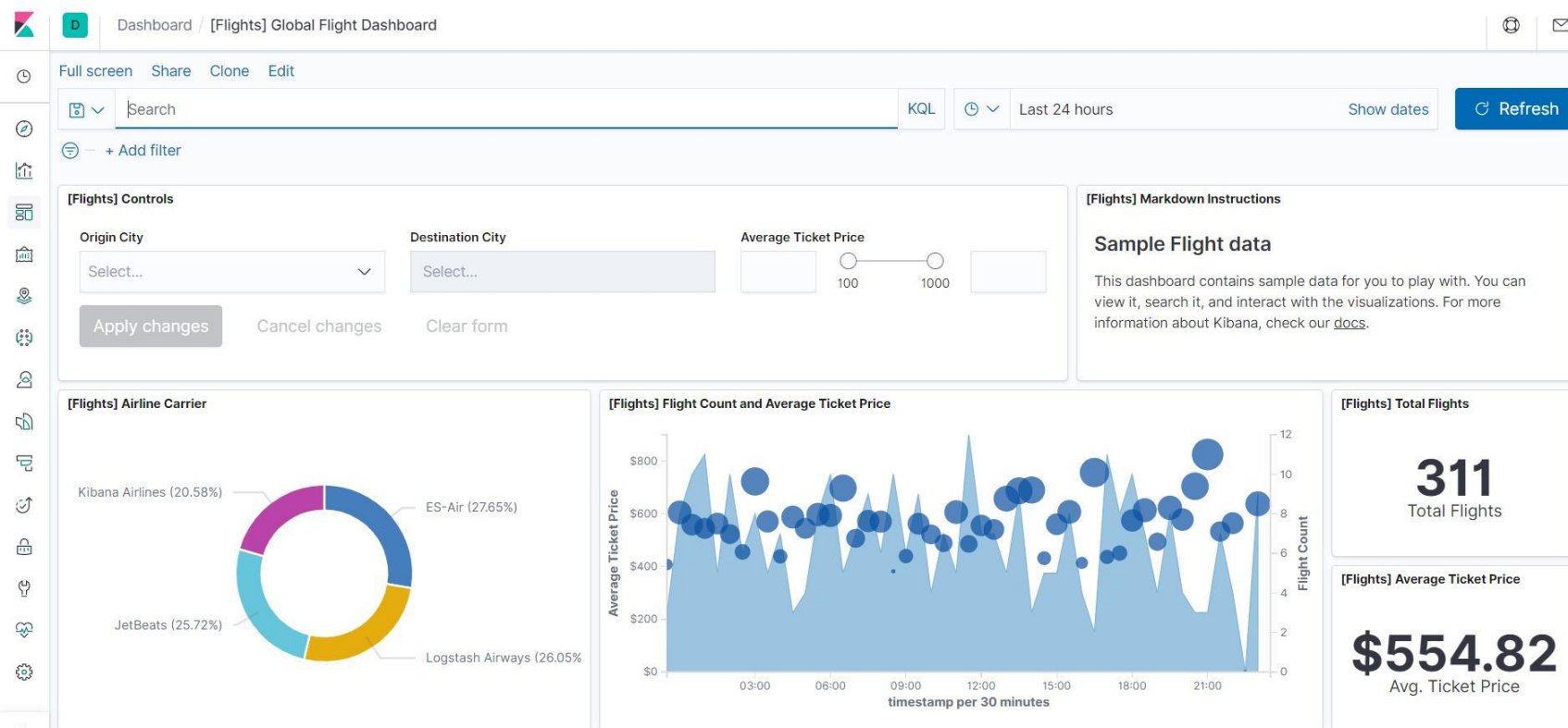




# داشبورد چیست و چه کاربردی دارد؟

۱. نمایش چندین نمودار همزمان

۲. یک دید کلی و جامع



# جشنواره عیدانه نیک آموز

از ۱۲ تا ۲۸ اسفند



برای کسب اطلاعات بیشتر به لینک زیر مراجعه کنید

[www.nikamooz.com/eyd1400](http://www.nikamooz.com/eyd1400)

# جشنواره عیدآموز نیک آموز

۳۰٪ تا ۵۰٪

تخفیف به همراه جوایز شگفت انگیز  
برای کسب اطلاعات بیشتر به لینک زیر مراجعه کنید

[www.nikamooz.com/eyd1400](http://www.nikamooz.com/eyd1400)

