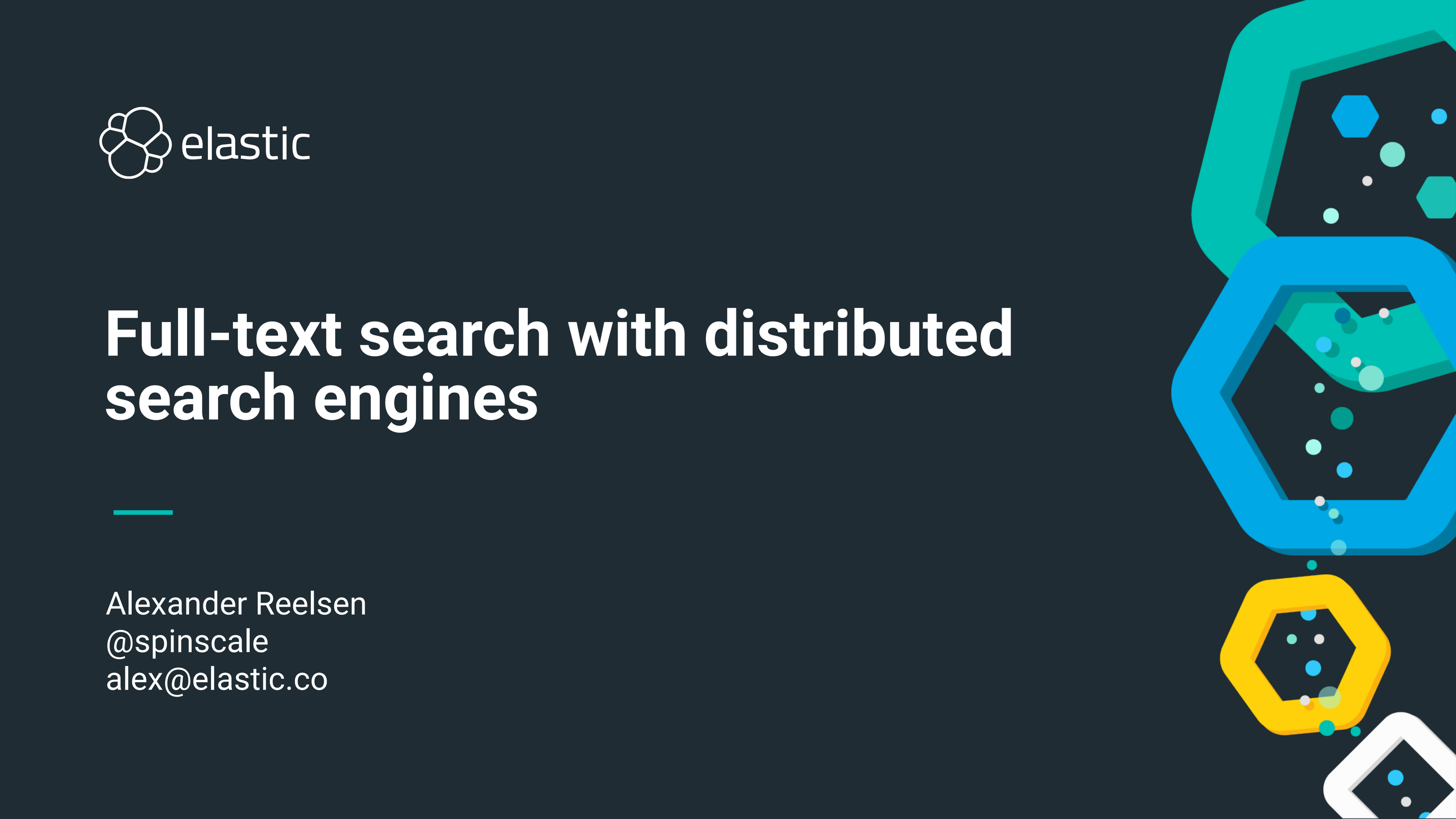


Full-text search with distributed search engines

Alexander Reelsen
@spinscale
alex@elastic.co

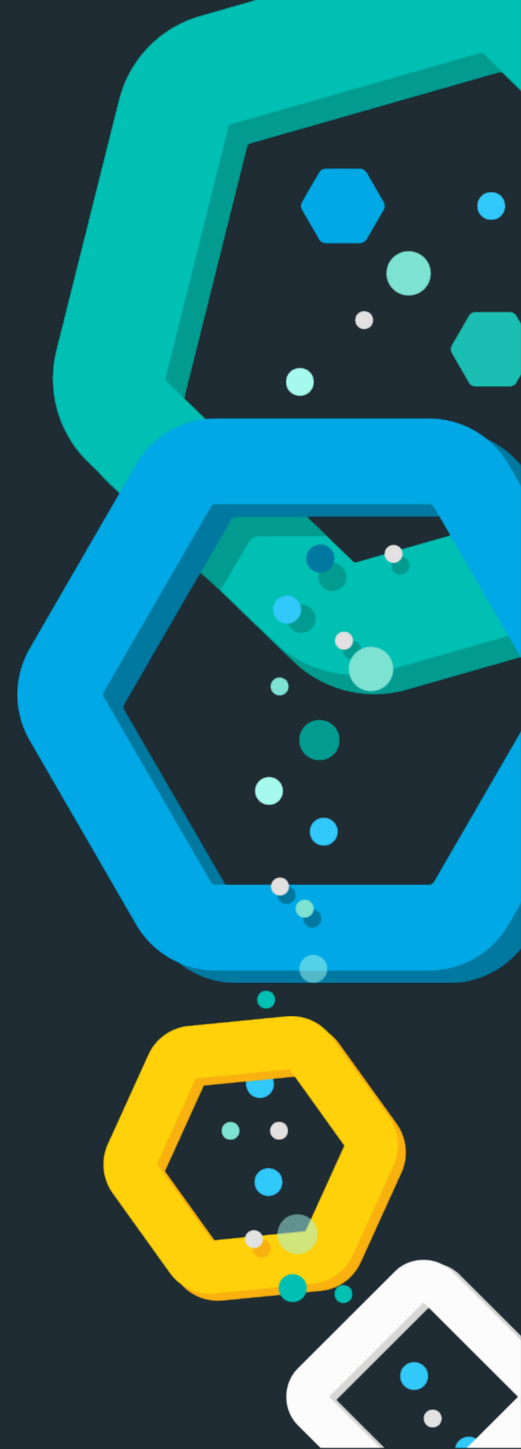
Agenda

- Overview
- Indexing: Analysis, Tokenization, Filtering, on disk data structures
- Searching: Scoring, Algorithms & Optimization
- Aggregations
- Distributed systems and search
- Q & A

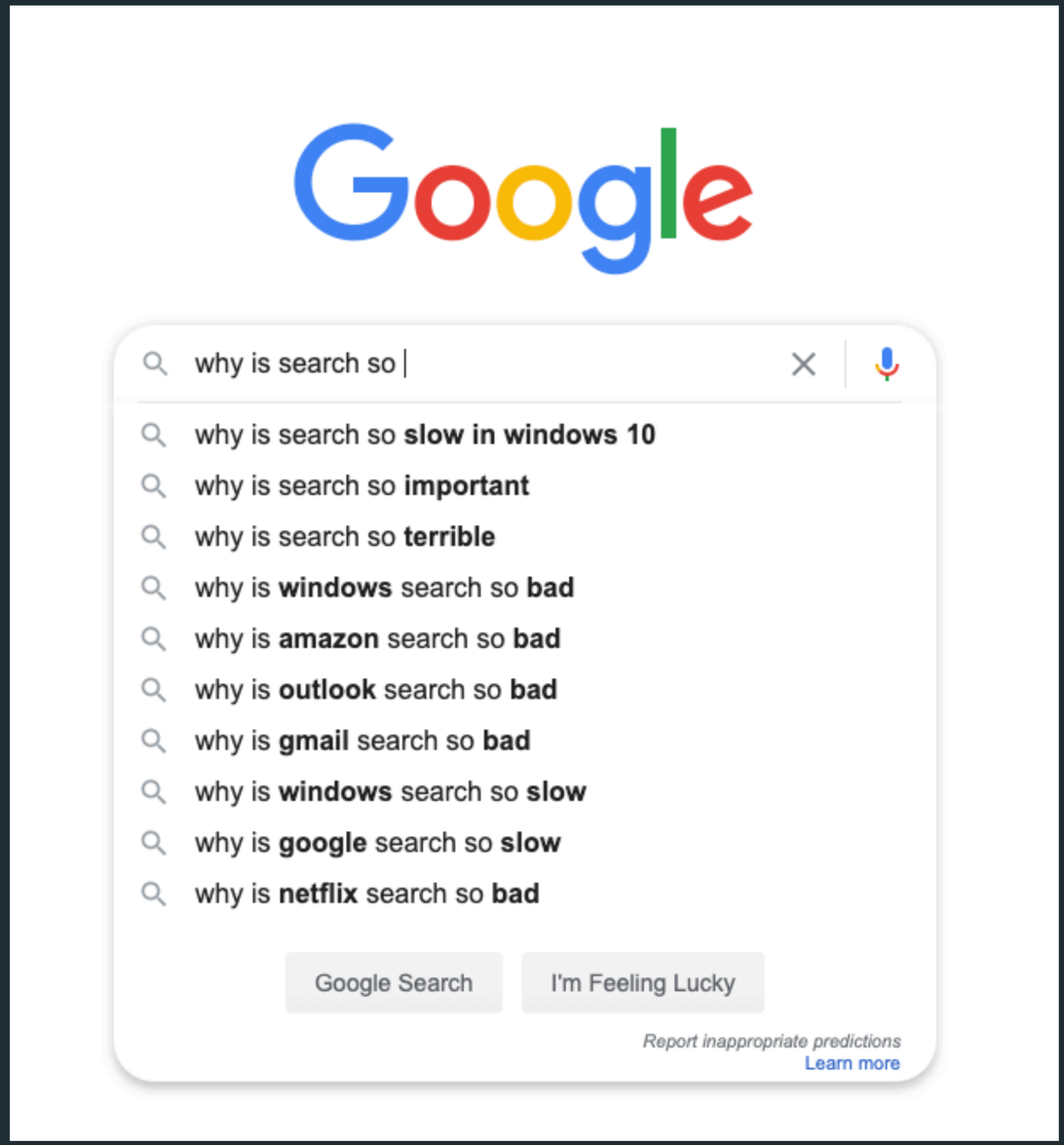
elastic

Overview

Full text search introduction



Why is search so important?



elastic

Repositories 25K
Code ?
Commits 467K
Issues 180K
Discussions Beta 35
Packages 30
Marketplace 1
Topics 72
Wikis 27K
Users 860

Languages

Python	4,861
Java	4,384
JavaScript	3,825
HTML	1,919
PHP	1,474
C++	830
CSS	754
C#	555
Jupyter Notebook	483
Ruby	477

Advanced search Cheat sheet

25,341 repository results

Sort: Best match

elastic/elasticsearch
Open Source, Distributed, RESTful **Search Engine**

java search-engine elasticsearch

☆ 50.2k Java Updated 3 minutes ago 213 issues need help

gigablast/open-source-**search-engine**
Nov 20 2017 -- A distributed open source **search engine** and spider/crawler written in C/C++ for Linux on Intel/AMD. Fr...

☆ 1.2k C++ Updated on 4 May

marcobiedermann/**search-engine**-optimization
A helpful checklist / collection of **Search Engine** Optimization (SEO) tips and techniques.

seo keyword optimization search google awesome collection engine tips awesome-list

☆ 1.5k HTML Updated 7 days ago

subins2000/**search**
An Open Source **Search Engine**

php search search-engine crawler

☆ 119 PHP Updated on 24 Jul 2017

mtianyan/FunpySpider**SearchEngine**
借鉴自慕课网【Scrapy 1.6.0爬取数据 + ElasticSearch6.8.0+Django2.2搜索引擎】

elasticsearch-analysis-ik mysql redis django elasticsearch python search-engine spider zhihu scrapy lagou

☆ 726 Python Apache-2.0 license Updated on 5 Apr

NeXTs/Jets.js
Native CSS **search engine**

css search-engine

☆ 2.8k JavaScript MIT license Updated on 7 Nov 2019

elastic

Home

PUBLIC

Stack Overflow

Tags

Users

FIND A JOB

Jobs

Companies

TEAMS What's this?

Free 30 Day Trial

Questions tagged [elasticsearch]

Ask Question

Elasticsearch is an Open Source (Apache 2), Distributed, RESTful, Search Engine based on Lucene.

Learn more... Top users Synonyms (1) elasticsearch jobs

45,757 questions

Newest | Active | Bountied 5 | Unanswered | More | Filter

0 votes
0 answers
5 views

Numeric range field versus 2 numeric fields

I have a elastic search index which has 2 fields, start timestamp and end timestamp. I am trying to do a intersect range query on it. I am now facing a dilemma where I wonder if I should make that a ...

elasticsearch lucene

asked 8 mins ago
Vinothkumar Raman
169 ● 7

0 votes
1 answer
9 views

Elastic Search Query using should is not working

I would like to filter my messages containing "No DB record found for Category:" or ""Not all codes match in DB for Category:". But the query returns all the messages that are ...

elasticsearch elasticsearch-5

asked 52 mins ago
iluvgarden
17 ● 6

0 votes
0 answers
15 views

Loading csv with unicode utf-8 into elasticsearch using python

i am trying to load csv file into elasticsearch using the code below. When running the code no failure is shown and once loading is done i try to access data in the localhost:9200 but i somehow cant ...

python csv elasticsearch

asked 9 hours ago
yolo25
35 ● 4

0 votes
1 answer
16 views

Elasticsearch - Point alias from OLD_INDEX to NEW_INDEX

I have an alias which is pointing to my OLD_INDEX. I have a requirement where I am creating a new index and after creation I need to point my alias A to the NEW_INDEX. I need to do this in Java. I ...

elasticsearch elasticsearch-7

asked 9 hours ago
newLearner
23 ● 5

The Overflow Blog

Podcast – 25 Years of Java: the past to the present

Java at 25: Features that made an impact and a look to the future

Featured on Meta

Improved experience for users with review suspensions

CEO Blog: Some exciting news about fundraising

Unnecessary secondary accounts and avoiding moderator action

2020 Community Moderator Election Results

Related Tags

kibana × 3633
logstash × 3593
java × 3512
nest × 2218
python × 1865
elastic-stack × 1559
lucene × 1524
c# × 1334
ruby-on-rails × 1188
json × 1142

more related tags

Hot Network Questions

WOMEN | MEN | KIDS

zalando

English Login Wish list Your bag

Get the Look NEW Clothing Shoes

hemd grün

Clothing
Shoes
Sport
Accessories
Premium
Care
Gift vouchers
Sale

'hemd grün'

Sort Size Brand Colour Price Material Delivery

2 items

GANT 99,99 €
GANT HERREN HEMD REGULAR ...

-56%

Andrew James ~~35,99 €~~
ANDREW JAMES HEMD - Shirt - gr... 15,99 €

Page 1 of 1

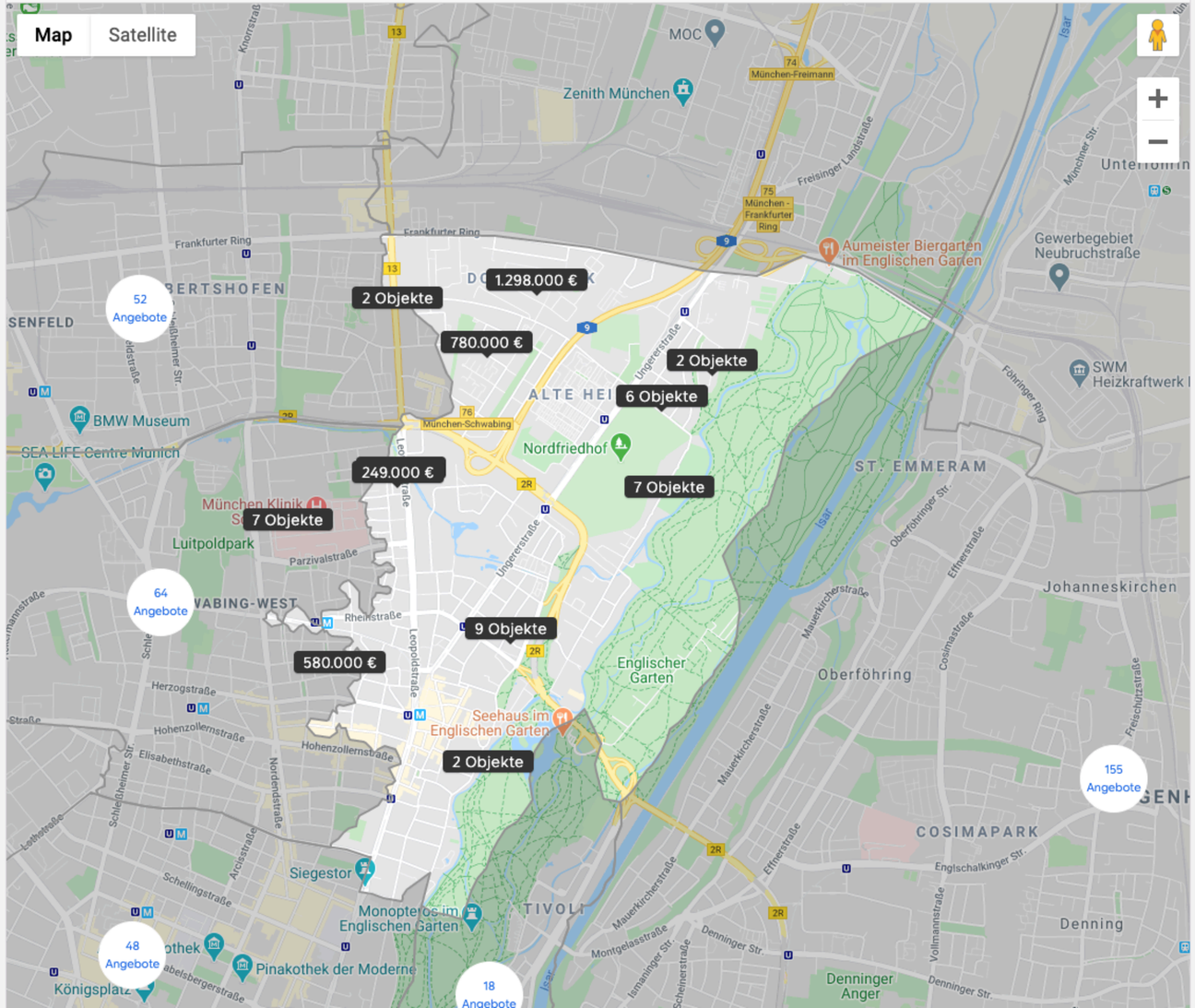
elastic

40 Eigentumswohnungen in Schwabing Suche speichern

Schwabing | Kaufpreis | Wohnfläche | Zimmer | Weitere Filter

Liste | Karte

Internet | Mobilfunk | Preise/m² | Wheelmap



elastic

yelp

indisches restaurant | München, Bayern

Für Unternehmen | Beitrag schreiben | Anmelden | Registrieren

Restaurants | Rund ums Haus | Rund ums Auto | Mehr

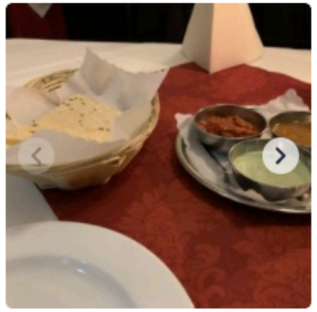
Top 10 indisches restaurant in München, Bayern

Sortieren: **Empfohlen**

Lieferservice 

Zum Abholen 

Alle | Preise | Jetzt geöffnet

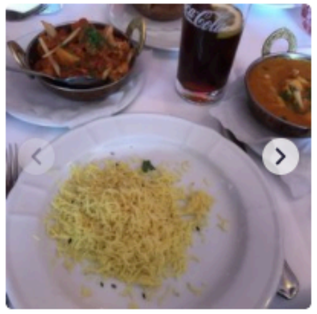


1. Natraj

111

€€ • Indisch

089 12001262
Nymphenburger Str. 26
Maxvorstadt

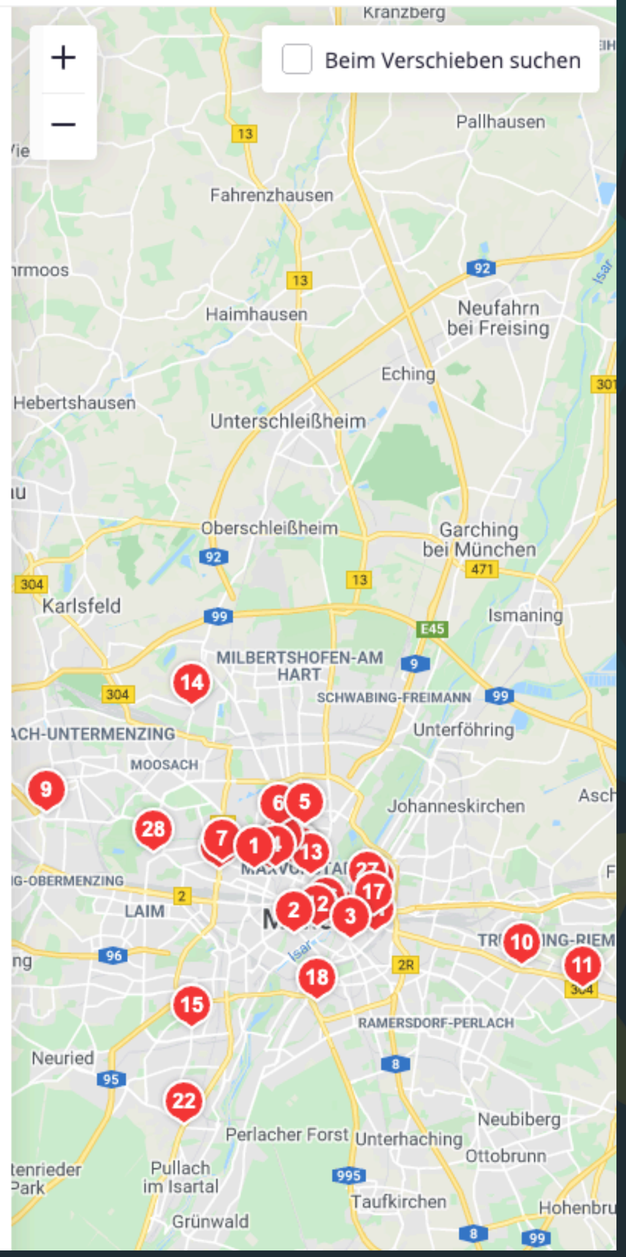


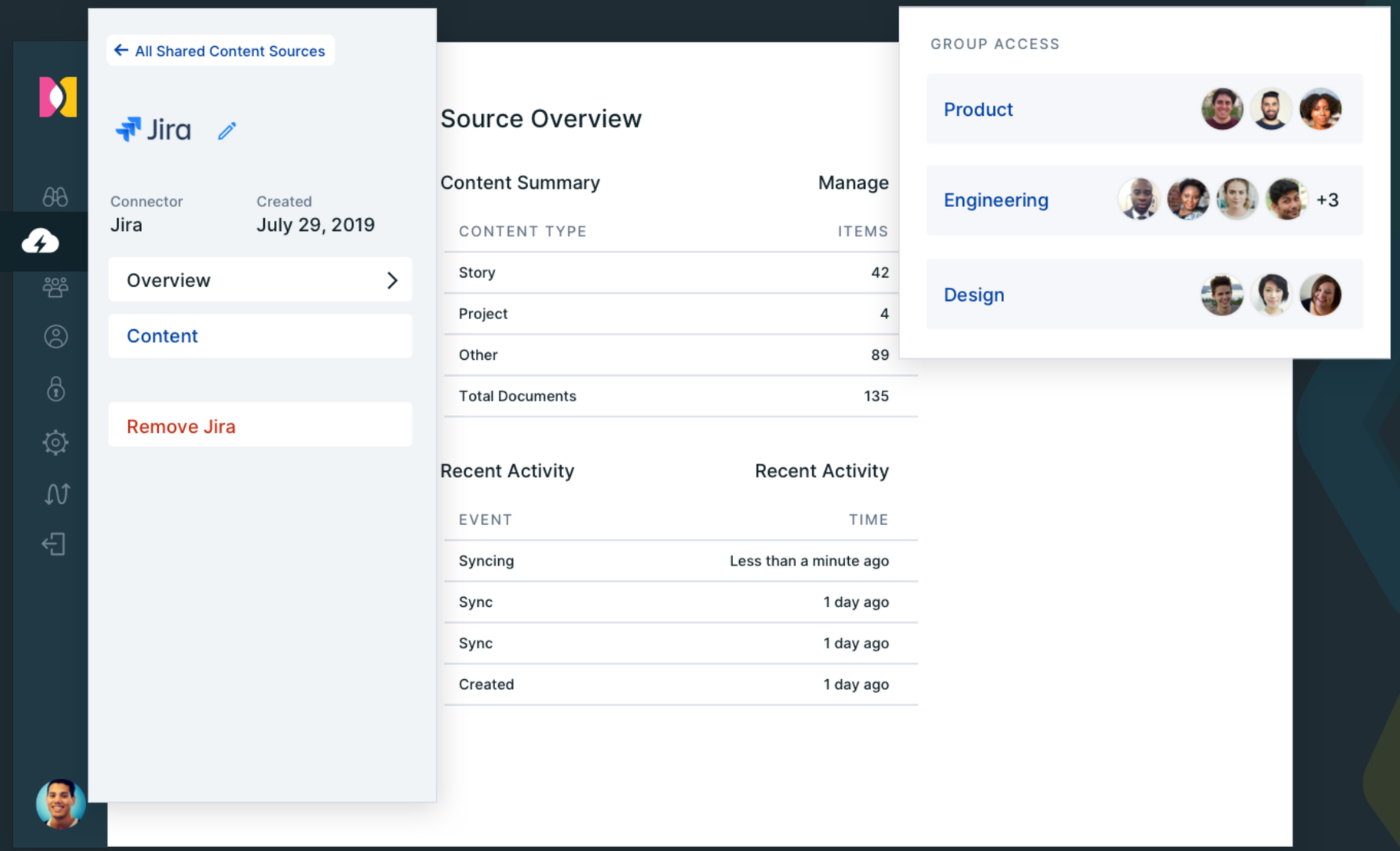
2. Palast der Winde

95

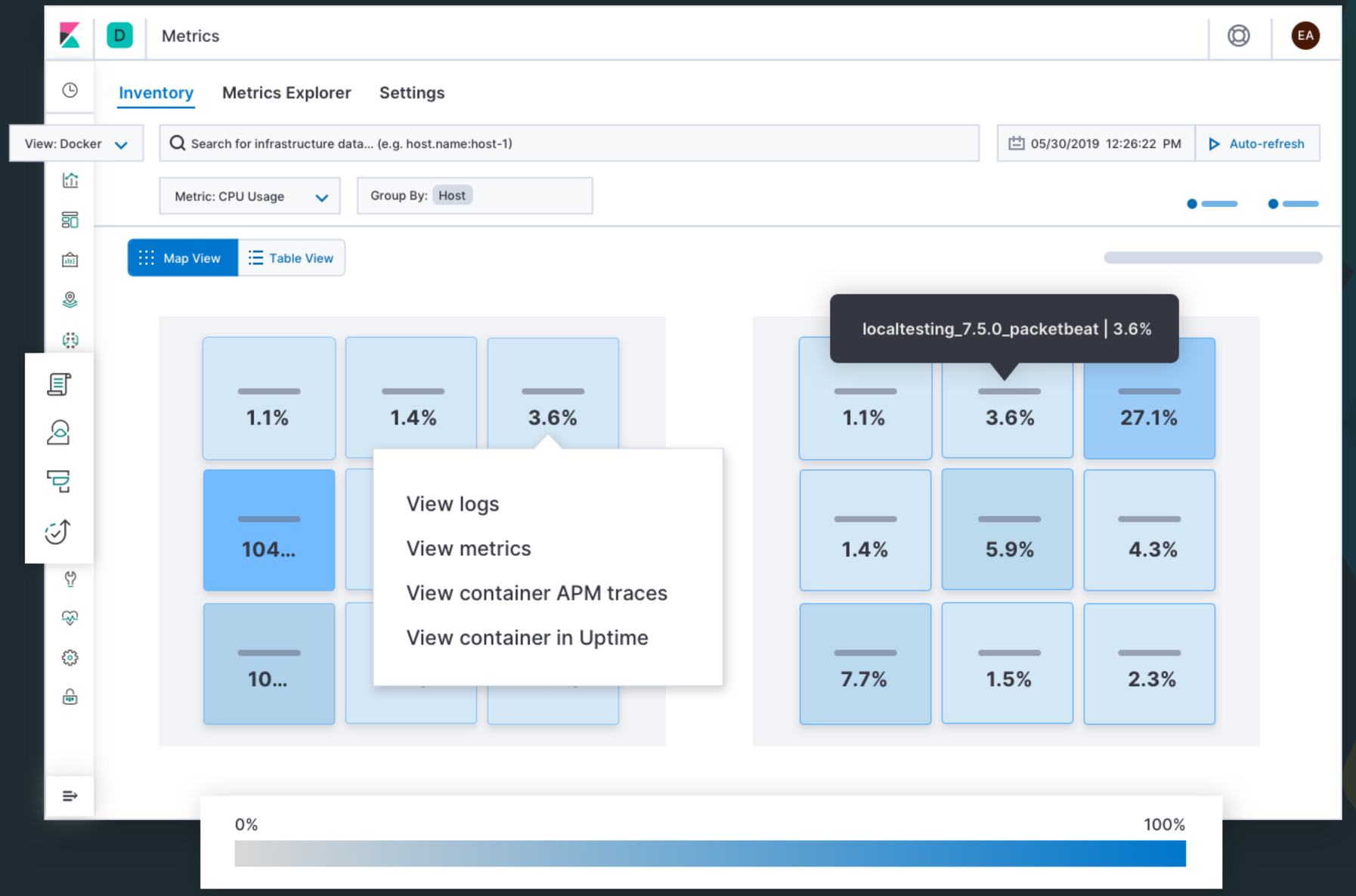
€€ • Indisch

089 263278
Hans-Sachs-Str. 8
Ludwigsvorstadt-Isarvorstadt

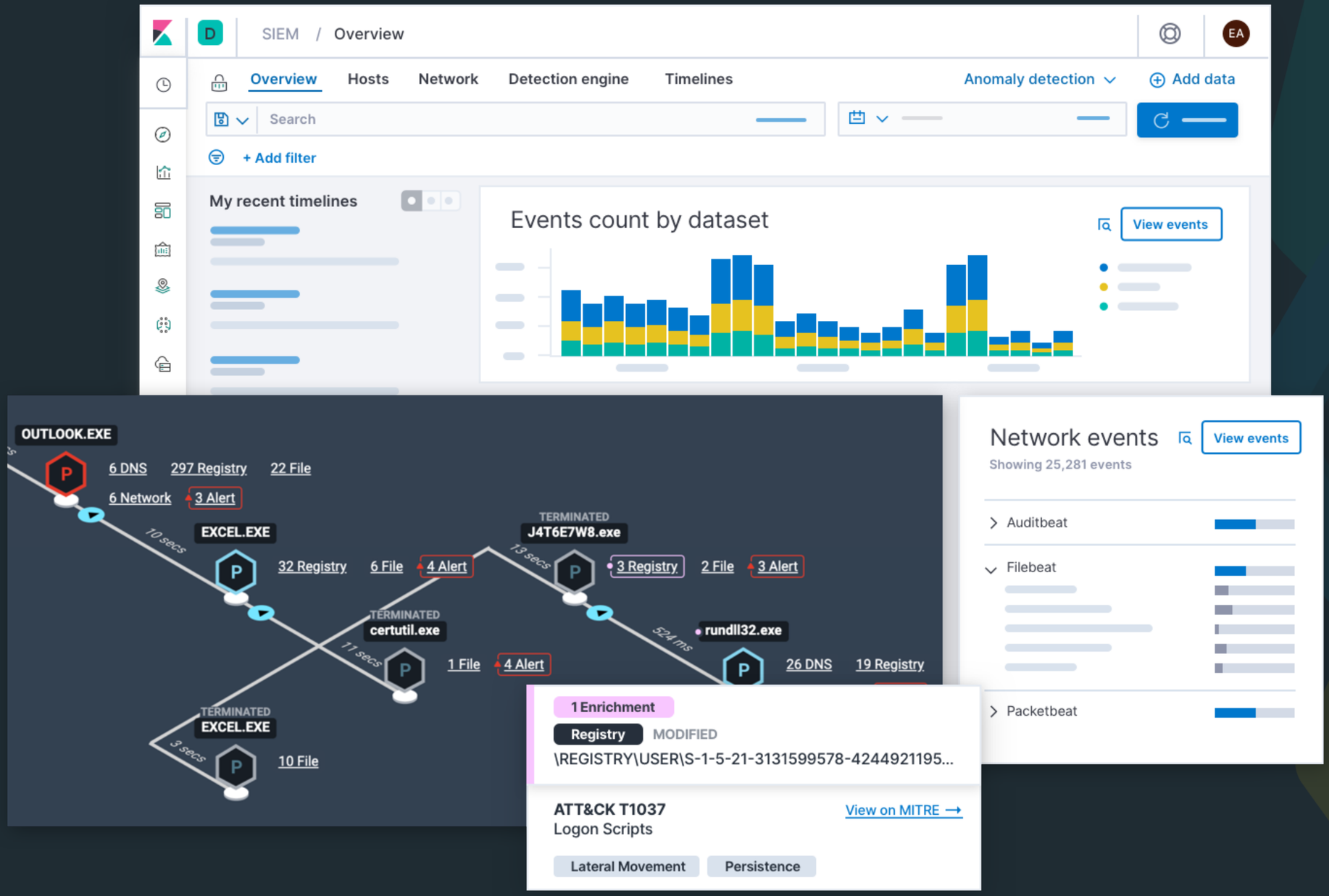



All Shared Content Sources
Jira
Connector
Jira
Created
July 29, 2019
Overview
Content
Remove Jira
Source Overview
Content Summary
Manage
CONTENT TYPE
ITEMS
Story
42
Project
4
Other
89
Total Documents
135
Recent Activity
Recent Activity
EVENT
TIME
Syncing
Less than a minute ago
Sync
1 day ago
Sync
1 day ago
Created
1 day ago
GROUP ACCESS
Product
Engineering
+3
Design

elastic


Metrics
EA
Inventory
Metrics Explorer
Settings
View: Docker
Search for infrastructure data... (e.g. host.name:host-1)
05/30/2019 12:26:22 PM
Auto-refresh
Metric: CPU Usage
Group By: Host
Map View
Table View
1.1%
1.4%
3.6%
104...
10...
View logs
View metrics
View container APM traces
View container in Uptime
localtesting_7.5.0_packetbeat | 3.6%
1.1%
3.6%
27.1%
1.4%
5.9%
4.3%
7.7%
1.5%
2.3%
0%
100%

elastic

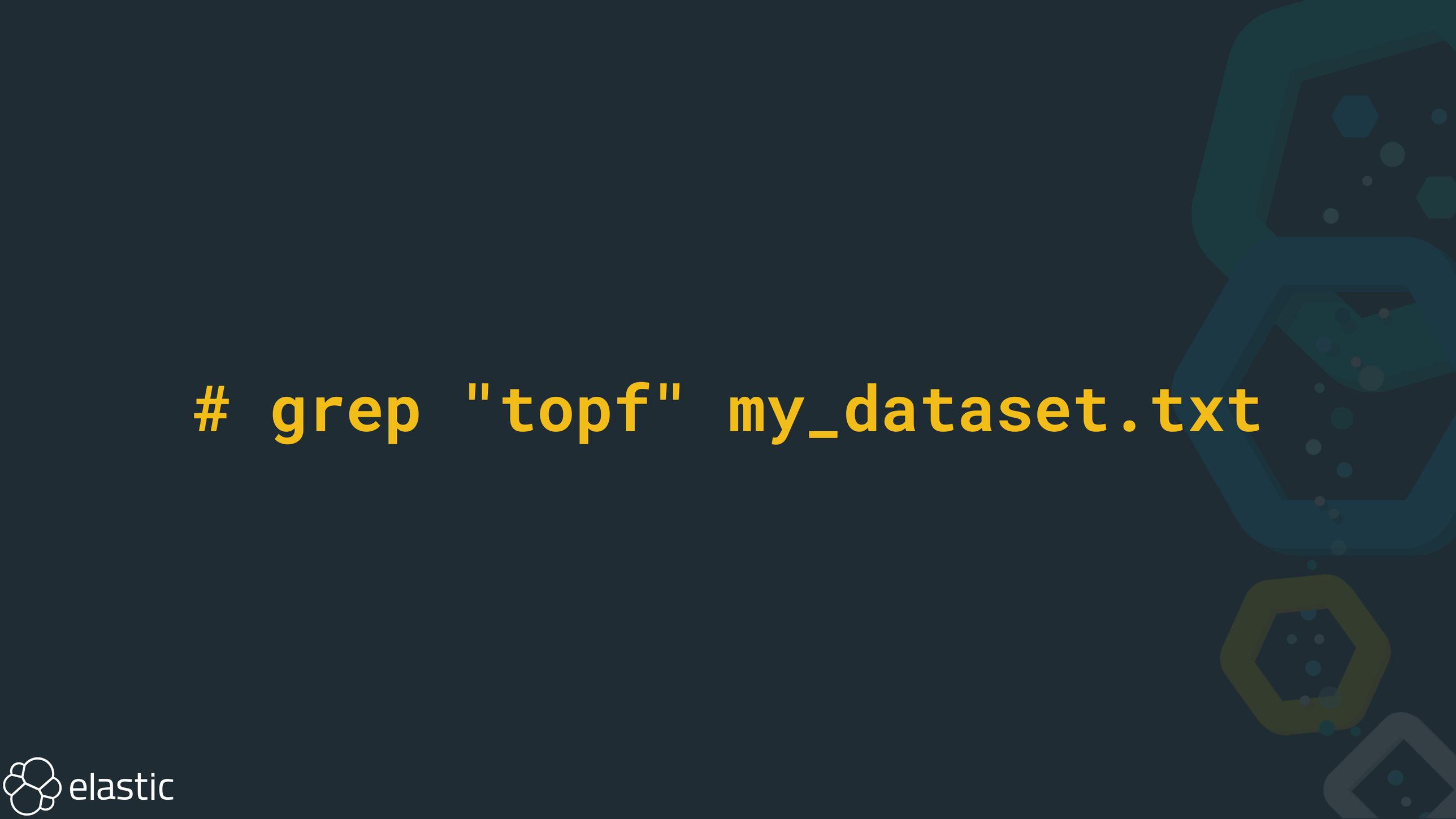

SIEM / Overview
EA
Overview
Hosts
Network
Detection engine
Timelines
Anomaly detection
Add data
Search
+ Add filter
My recent timelines
Events count by dataset
View events
OUTLOOK.EXE
6 DNS
297 Registry
22 File
6 Network
3 Alert
10 secs
EXCEL.EXE
32 Registry
6 File
4 Alert
TERMINATED
J4T6E7W8.exe
13 secs
3 Registry
2 File
3 Alert
TERMINATED
certutil.exe
11 secs
1 File
4 Alert
524 ms
rundll32.exe
26 DNS
19 Registry
TERMINATED
EXCEL.EXE
3 secs
10 File
Network events
View events
Showing 25,281 events
Auditbeat
Filebeat
Packetbeat
1 Enrichment
Registry
MODIFIED
\REGISTRY\USER\S-1-5-21-3131599578-4244921195...
ATT&CK T1037
Logon Scripts
View on MITRE
Lateral Movement
Persistence

elastic

```
SELECT * FROM products
         WHERE name LIKE = '%topf%'
```

elastic

```
# grep "topf" my_dataset.txt
```



elastic

Problem

- Scales linearly with the data set size
- Relevancy
- Spell correction
- Synonyms
- Phrases

Inverted Index

elastic

The quick brown fox jumped over the lazy dog

Tokenize

The	1
quick	1
brown	1
fox	1
jumped	1
over	1
the	1
lazy	1
dog	1

Sort

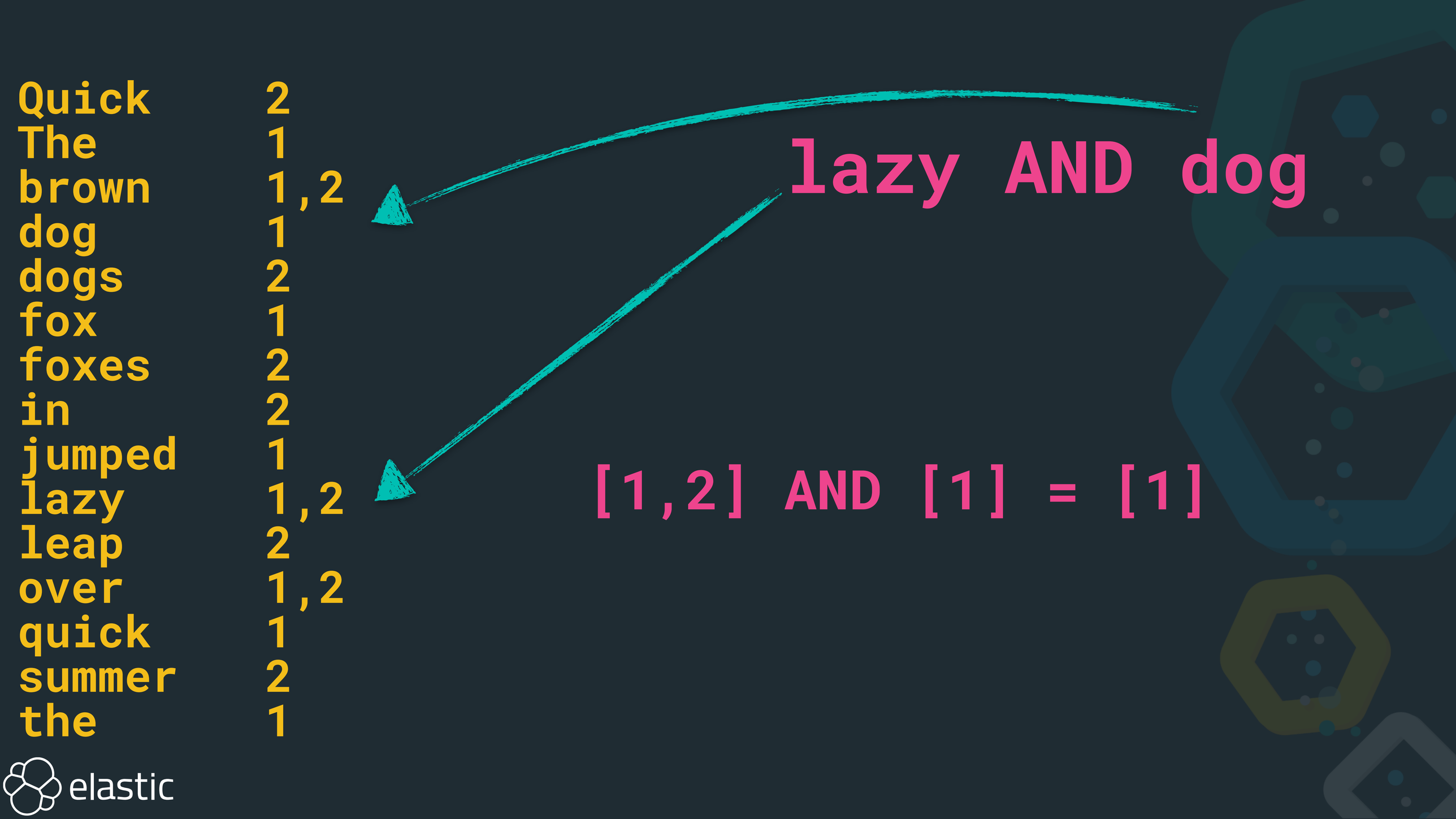
The	1
brown	1
dog	1
fox	1
jumped	1
lazy	1
over	1
quick	1
the	1

Quick brown foxes leap over lazy dogs in summer

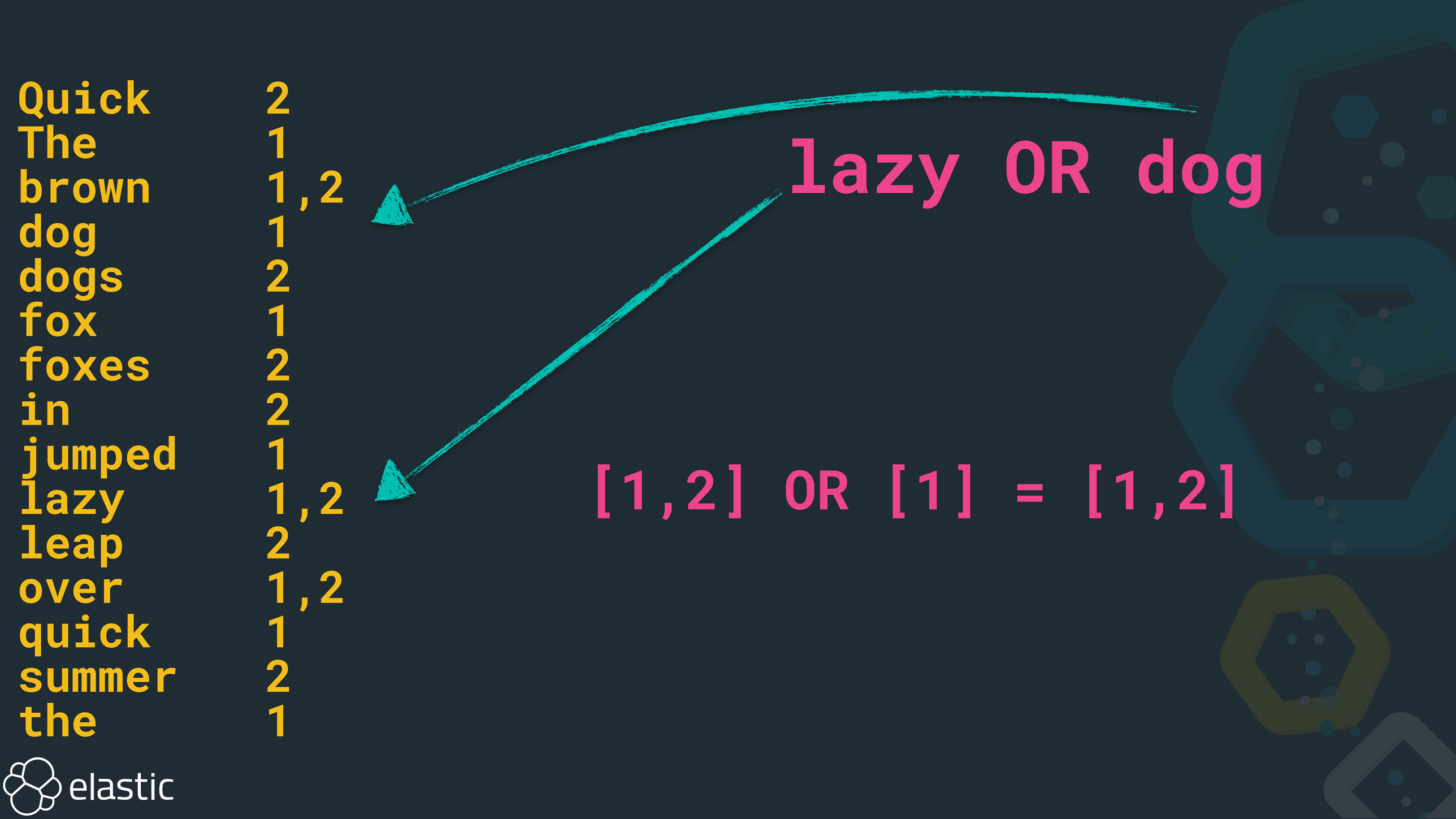
elastic

Quick	2
The	1
brown	1,2
dog	1
dogs	2
fox	1
foxes	2
in	2
jumped	1
lazy	1,2
leap	2
over	1,2
quick	1
summer	2
the	1

Quick	2
The	1
brown	1,2
dog	1
dogs	2
fox	1
foxes	2
in	2
jumped	1
lazy	1,2
leap	2
over	1,2
quick	1
summer	2
the	1


Quick 2
The 1
brown 1,2
dog 1
dogs 2
fox 1
foxes 2
in 2
jumped 1
lazy 1,2
leap 2
over 1,2
quick 1
summer 2
the 1
lazy AND dog
[1,2] AND [1] = [1]

elastic


Quick 2
The 1
brown 1,2
dog 1
dogs 2
fox 1
foxes 2
in 2
jumped 1
lazy 1,2
leap 2
over 1,2
quick 1
summer 2
the 1
lazy OR dog
[1,2] OR [1] = [1,2]

elastic

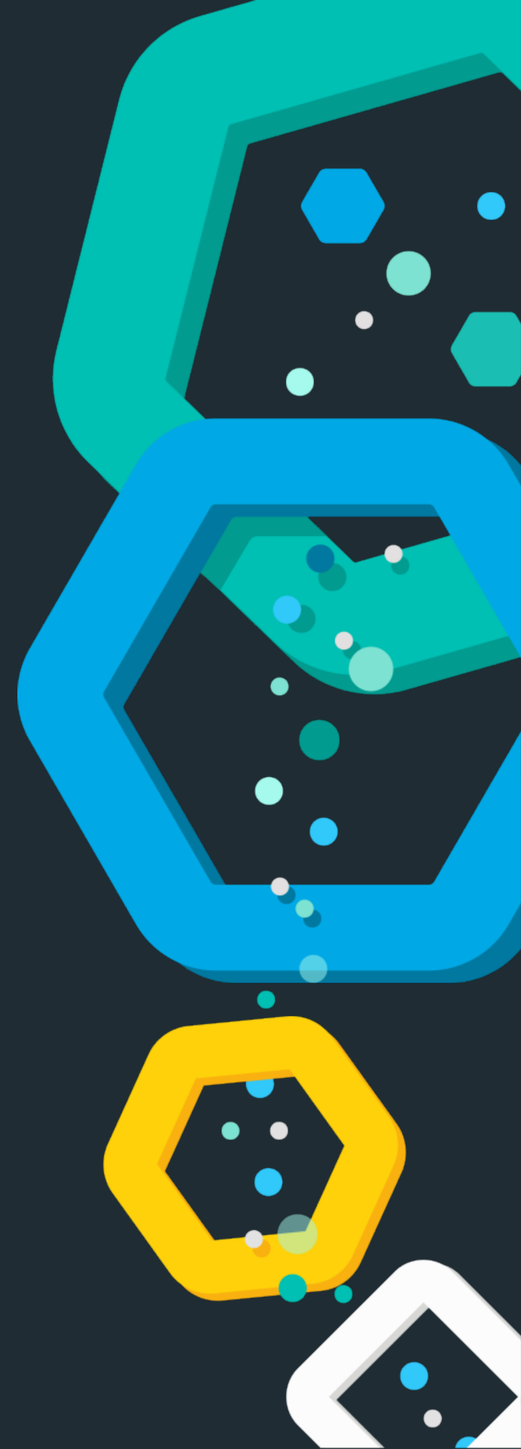
Technologies used today

- Apache Lucene (search library)
- Elasticsearch (distributed search engine built on top of Apache Lucene)

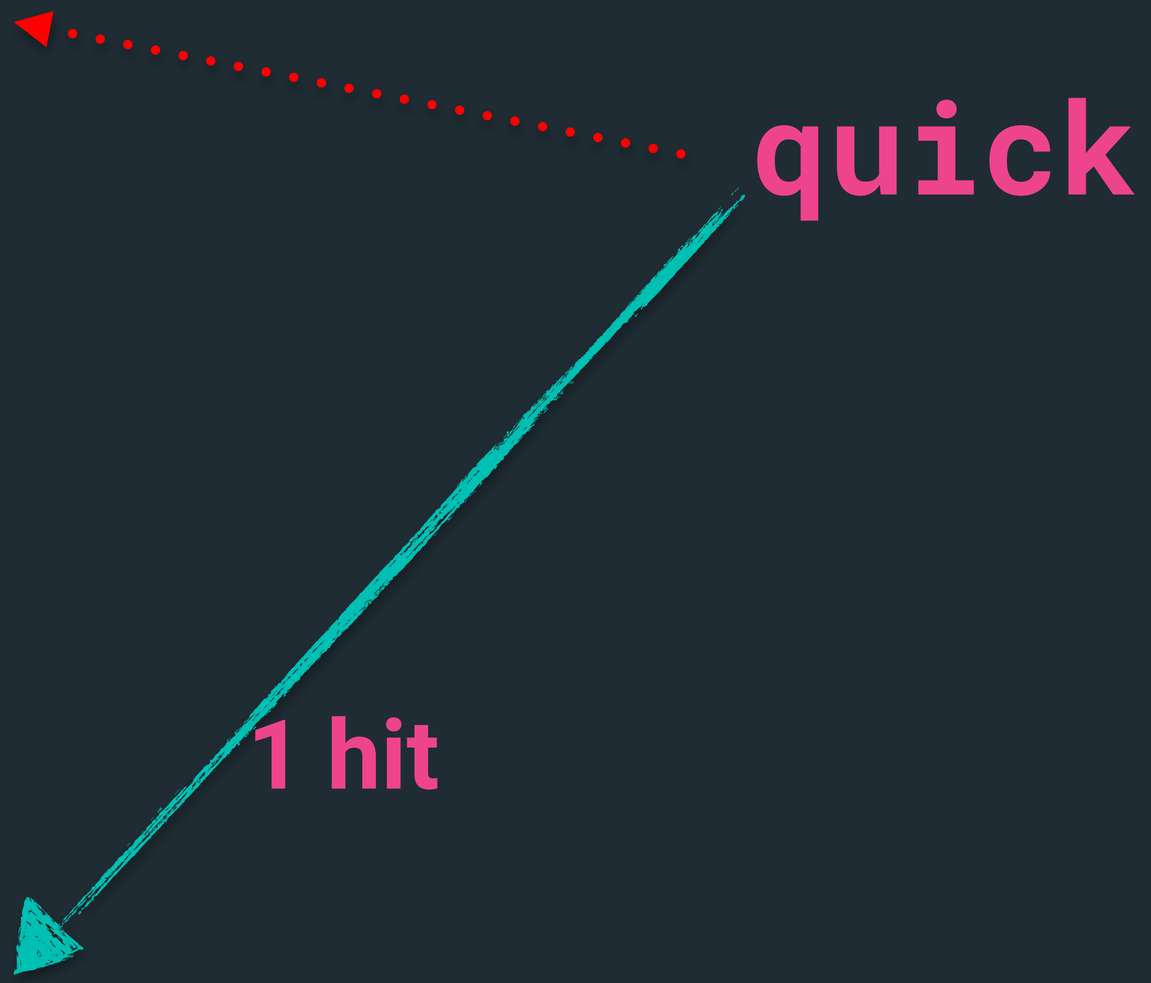
elastic

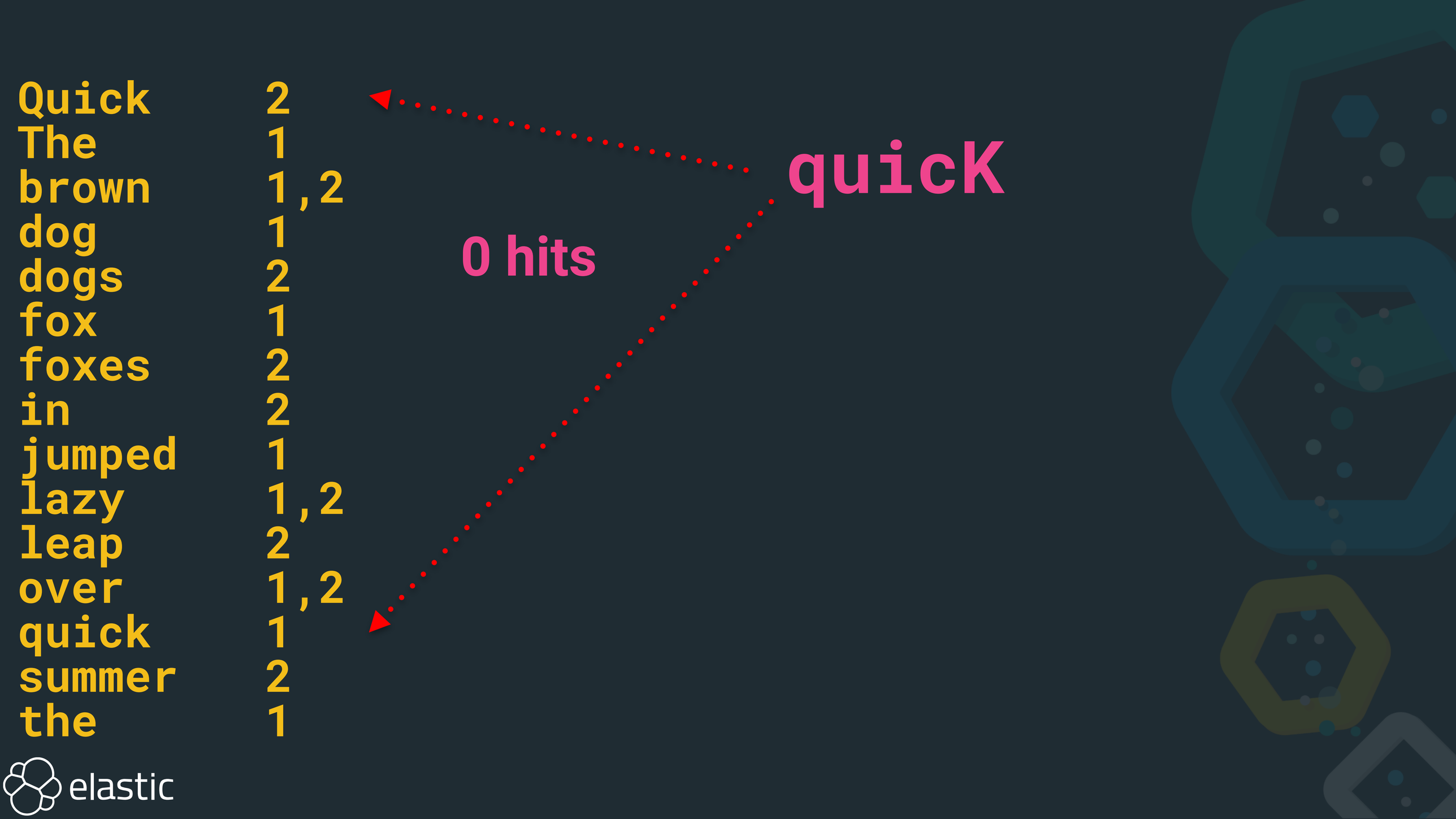
Indexing

Analysis, Tokenization, Filtering
Data structures



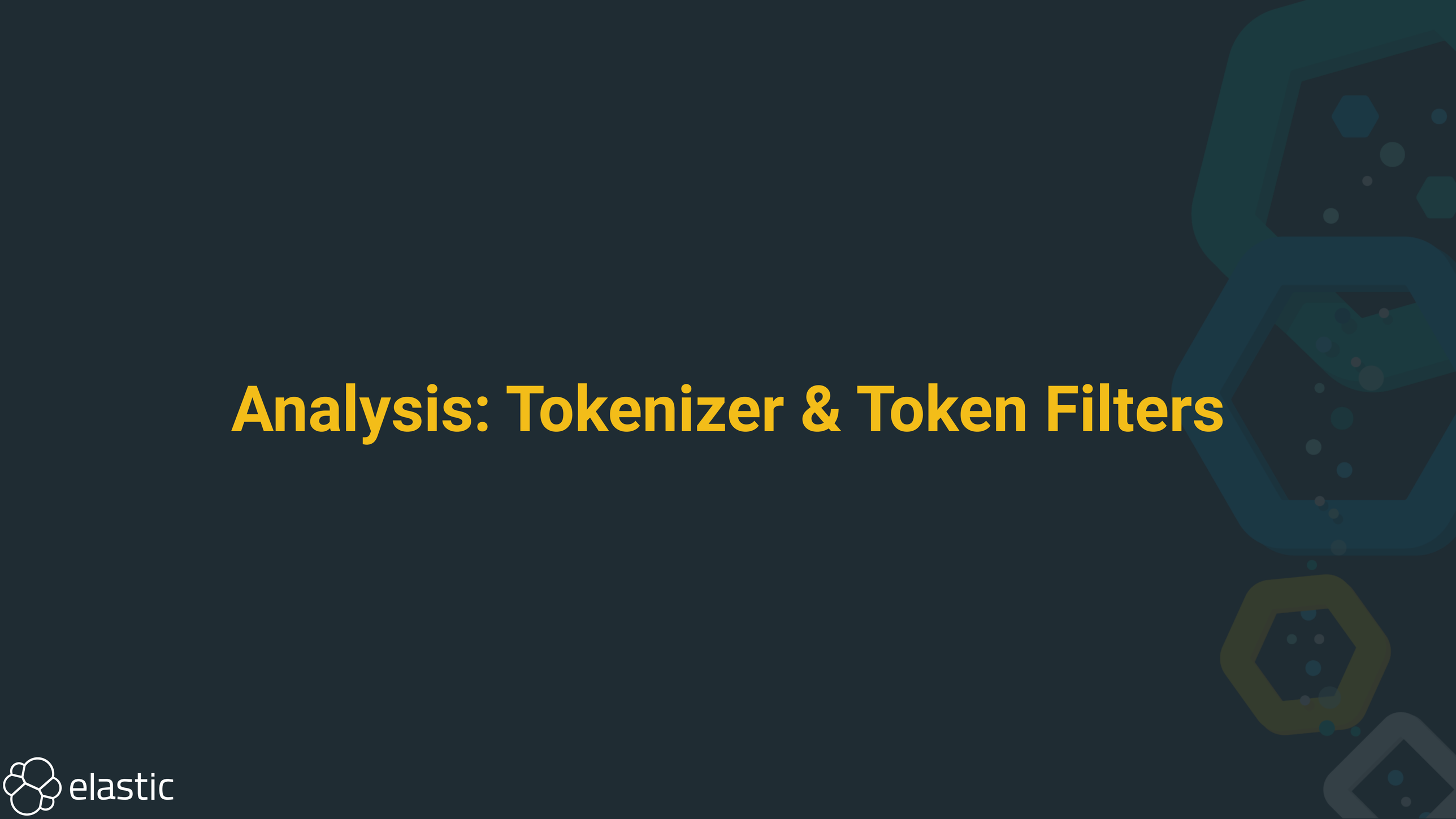
Quick	2
The	1
brown	1,2
dog	1
dogs	2
fox	1
foxes	2
in	2
jumped	1
lazy	1,2
leap	2
over	1,2
quick	1
summer	2
the	1




Quick 2
The 1
brown 1,2
dog 1
dogs 2
fox 1
foxes 2
in 2
jumped 1
lazy 1,2
leap 2
over 1,2
quick 1
summer 2
the 1
quicK
0 hits

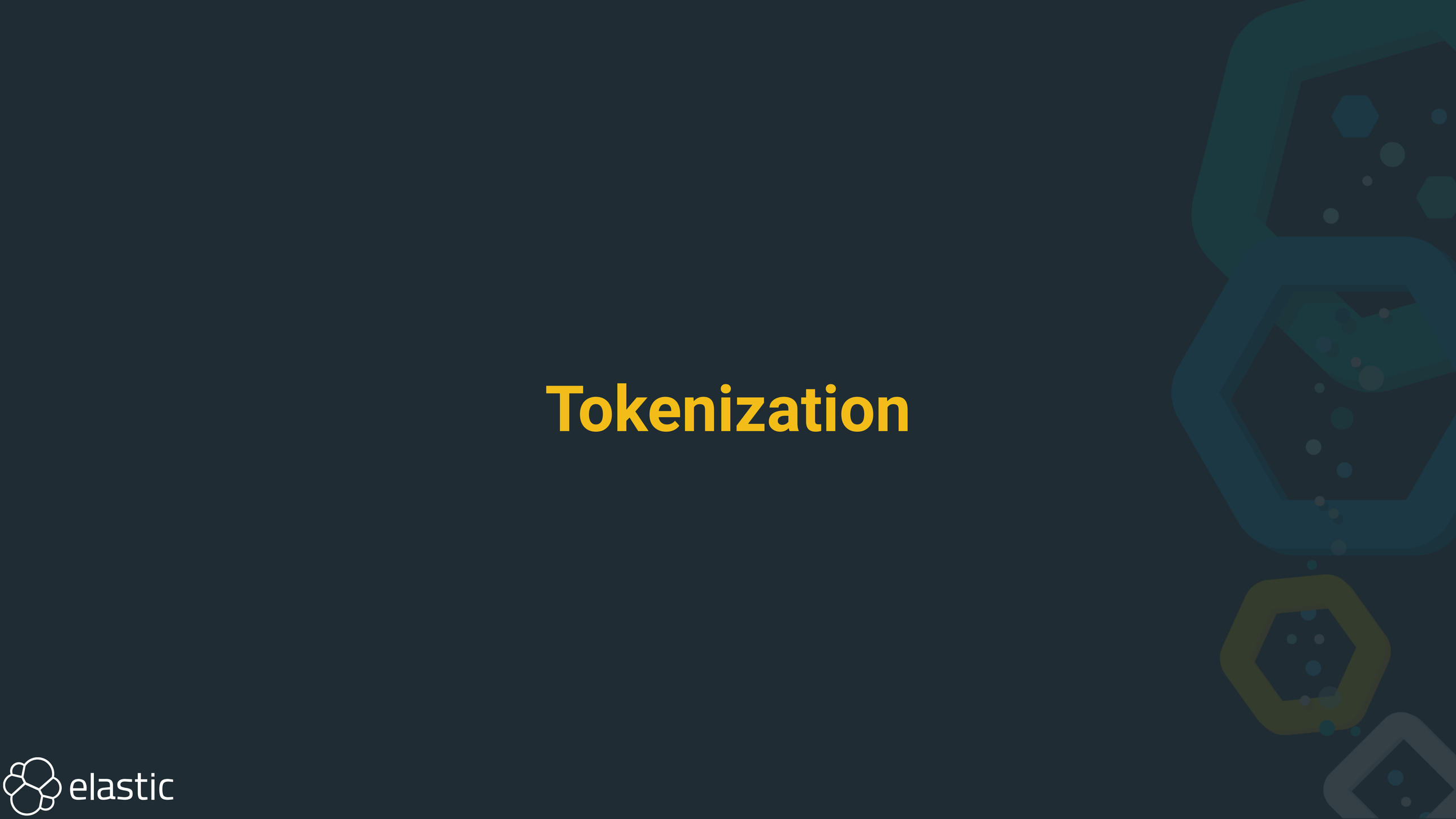
elastic

Analysis: Tokenizer & Token Filters



elastic

Tokenization



elastic

Tokenization

```
quick brown fox
```

Tokenization

```
quick_brown_fox
```

elastic

Tokenization

```
quick_brown_fox
the lazy, white dog.
```

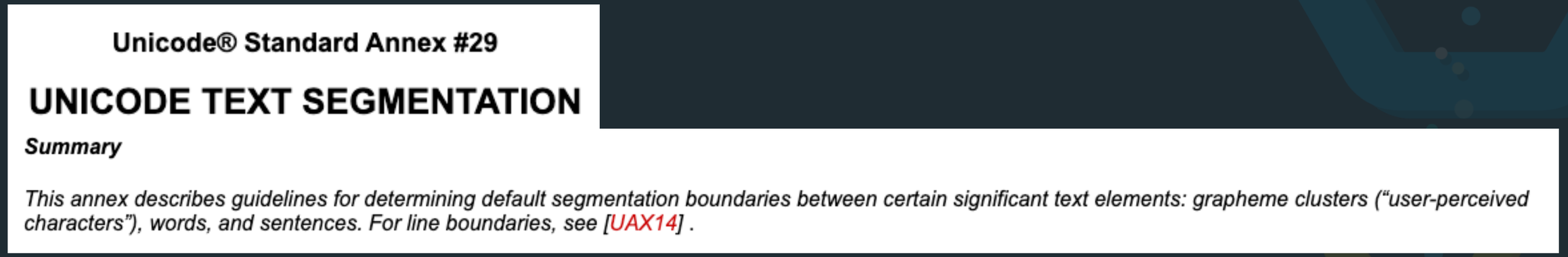
elastic

Tokenization

```
quick_brown_fox
the_lazy_white_dog
```

Tokenization

```
quick_brown_fox
the_lazy_white_dog
```



Unicode® Standard Annex #29

UNICODE TEXT SEGMENTATION

Summary

This annex describes guidelines for determining default segmentation boundaries between certain significant text elements: grapheme clusters (“user-perceived characters”), words, and sentences. For line boundaries, see [UAX14] .

https://unicode.org/reports/tr29/

elastic

Tokenization

```
quick_brown_fox
the_lazy_white_dog
https://www.jade-hs.de
```

Tokenization

```
quick_brown_fox
the_lazy_white_dog
https_www.jade_hs.de
```

elastic

Token Filter

elastic

Quick	2
The	1
brown	1,2
dog	1
dogs	2
fox	1
foxes	2
in	2
jumped	1
lazy	1,2
leap	2
over	1,2
quick	1
summer	2
the	1

Token filter

Token filter

Lowercase

elastic

Token filter

	Lowercase	Stopwords
The	the	
Quick	quick	quick
brown	brown	brown
fox	fox	fox

Token filter

	Lowercase	Stopwords	Synonyms
The Quick brown fox	the quick brown fox	quick brown fox	quick,fast brown fox

Token filter

	Lowercase	Stopwords	Synonyms
The Quick brown fox	the quick brown fox	quick brown fox	quick,fast brown fox

Tokens can be changed, added, removed

elastic

Token filter

	Lowercase	Stopwords	Synonyms
The	the		
Quick	quick	quick	quick,fast
brown	brown	brown	brown
fox	fox	fox	fox

Queries need to be processed as well!

More analysis strategies

- Phonetic analysis: `Meyer vs. Meier`
- Stemming: `foxes → fox`
- Compounding: `Blumentopf → blumen topf`
- Folding: `Spaß → Spass`

(On-Disk) Data structures

elastic

What else is in an inverted index?

- Documents: Find documents
- Term frequencies: Relevancy
- Positions: Positional Queries
- Offsets: Highlighting
- Stored fields: The original data

Segment: Unit of work

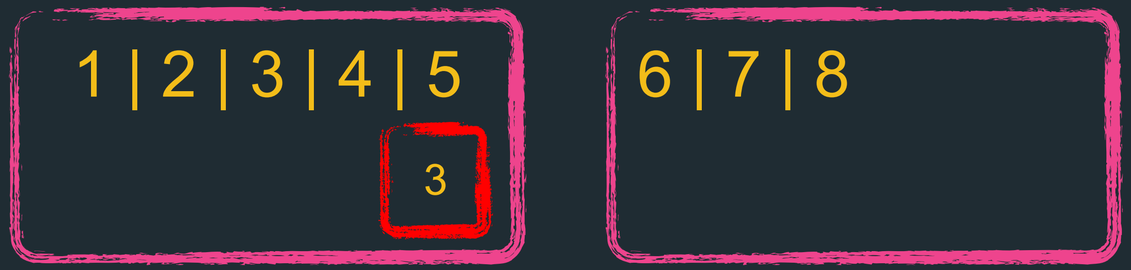
- A fully self sufficient inverted index
- An index consists of a number of segments
- New segments are created for newly added documents
- Segments are immutable!

Read-only data structures

- Pro: Write-once, sequentially
- Pro: Lock-free reading
- Pro: File system cache
- Contra: in-place updates & deletes
- Contra: Housekeeping
- Contra: Transactions

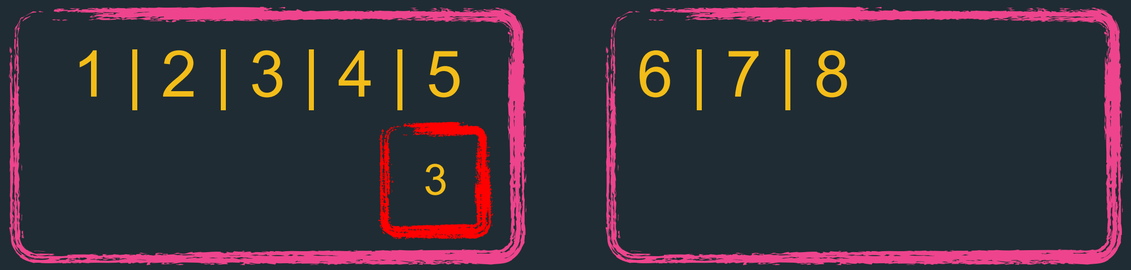
Segment: Deletes

- Mark a document as deleted in a special file
- Exclude it from searches
- No space is freed!



Segment: Merging

- Number of segments needs to be kept reasonable
- Merge multiple segments into one (smaller index)
- Delete expired documents



elastic

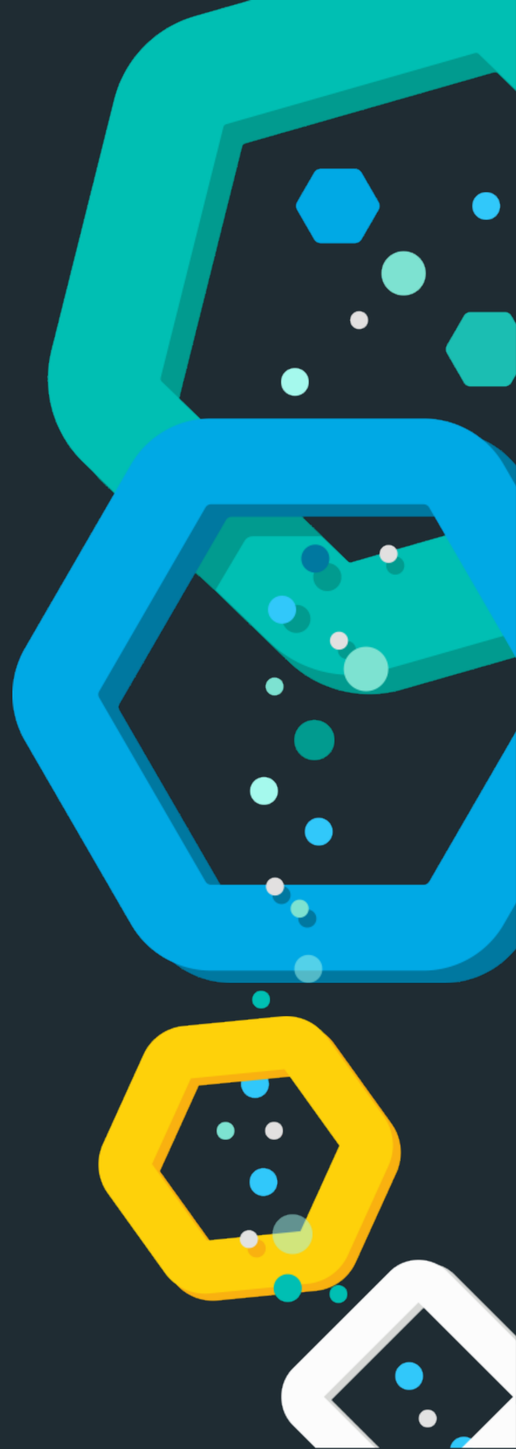
Segment: Merging

- Number of segments needs to be kept reasonable
- Merge multiple segments into one (smaller index)
- Delete expired documents

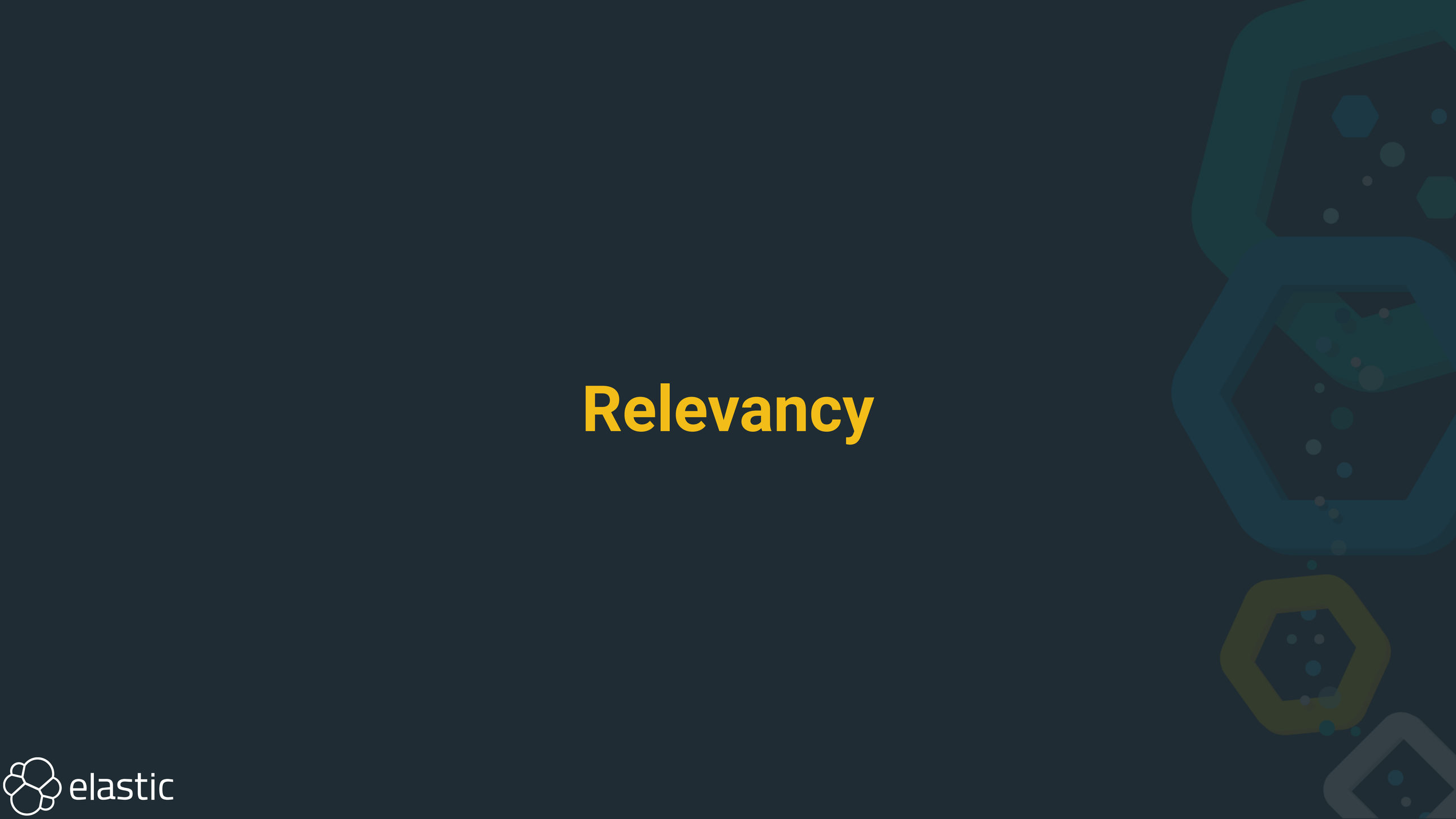
elastic

Searching

Precision vs. recall
Scoring
Algorithms and optimizations



Relevancy

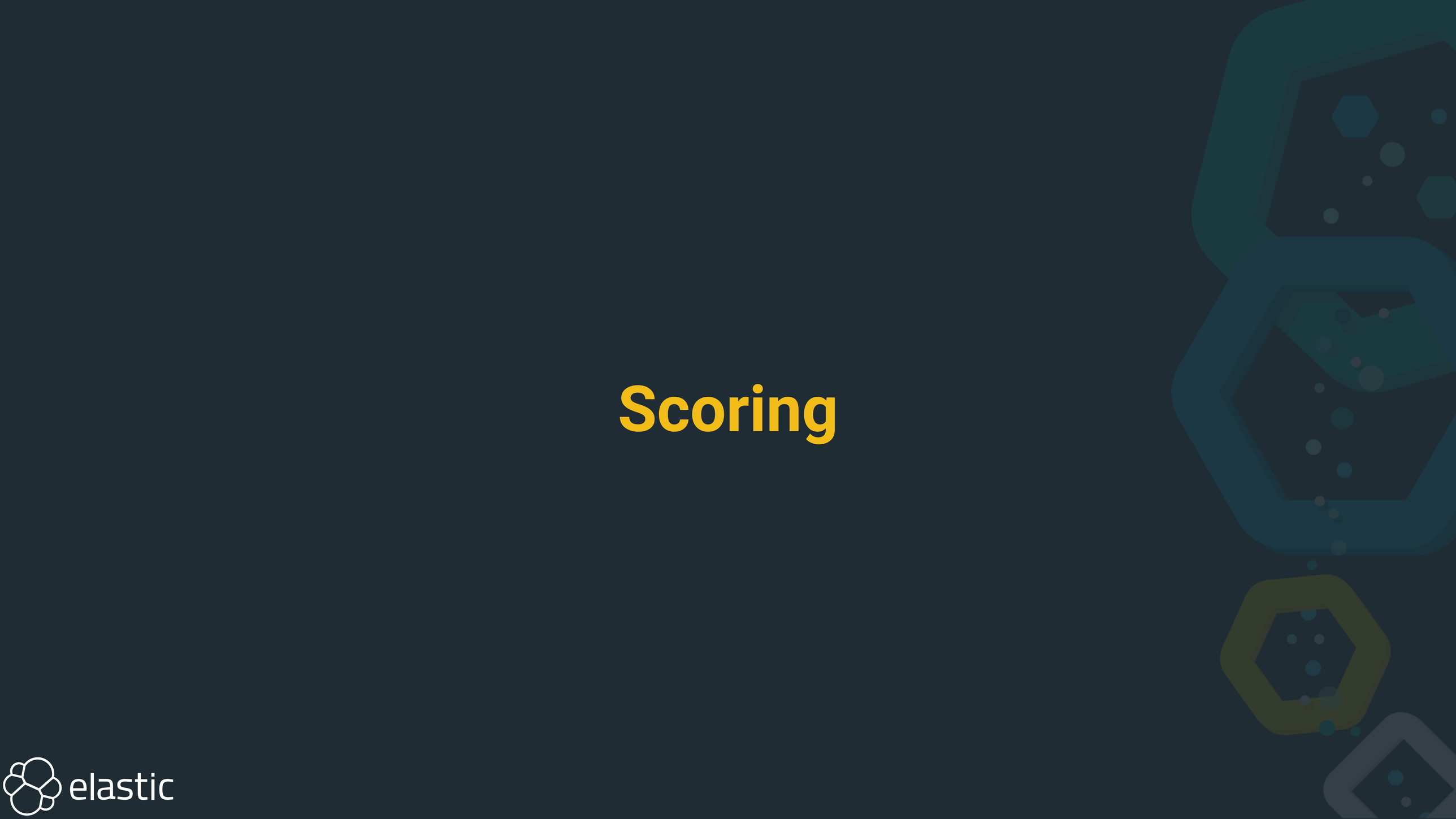


elastic

Relevancy

- Textbook answer: How well matches a document a query?
- Business answer: Are the top search results those that make me the most money?
  - marketplace
  - hotel booking website
  - newspaper website

Scoring



elastic

Scoring: `lazy dog`

- Naive: increase a counter if a term is matched
- "the lazy dog" => score 2
- "the lazy frog" => score 1
- "the lazy lazy lazy lazy cat" => score 4 or 1?

Scoring: More than term frequency

- How about incorporating information about the whole document corpus in scoring?
- Are lesser common terms more relevant?
- news paper: `"dieselgate news"`

Scoring: TF-IDF

- Term frequency: number of times a term occurs in a field
- Inverse document frequency: inverse function of the number of documents in which it occurs

Scoring: Vector space model

- Each term is a dimension
- The length is based on tf-idf calculation
- Similarity is the angle between vectors
- Cosine similarity: best match == angle 0°

Scoring: TF-IDF in Lucene

$$score(q,d) = \sum (tf(t \text{ in } d) \cdot idf(t)^2 \cdot t.getBoost() \cdot norm(t,d))$$

Lucene's Practical Scoring Function is derived from the above. The color codes demonstrate how it relates to those of the *conceptual* formula:

$$\text{score}(q,d) = \sum_{t \text{ in } q} \left(\text{tf}(t \text{ in } d) \cdot \text{idf}(t)^2 \cdot \text{t.getBoost}() \cdot \text{norm}(t,d) \right)$$

Lucene Practical Scoring Function

where

1. ***tf(t in d)*** correlates to the term's *frequency*, defined as the number of times term *t* appears in the currently scored document *d*. Documents that have more occurrences of a given term receive a higher score. Note that *tf(t in q)* is assumed to be *1* and therefore it does not appear in this equation, However if a query contains twice the same term, there will be two term-queries with that same term and hence the computation would still be correct (although not very efficient). The default computation for *tf(t in d)* in `ClassicSimilarity` is:

$$\texttt{tf(t in d)} = \text{frequency}^{1/2}$$

2. ***idf(t)*** stands for Inverse Document Frequency. This value correlates to the inverse of *docFreq* (the number of documents in which the term *t* appears). This means rarer terms give higher contribution to the total score. *idf(t)* appears for *t* in both the query and the document, hence it is squared in the equation. The default computation for *idf(t)* in `ClassicSimilarity` is:

$$\texttt{idf(t)} = 1 + \log\left(\frac{\text{docCount}+1}{\text{docFreq}+1}\right)$$

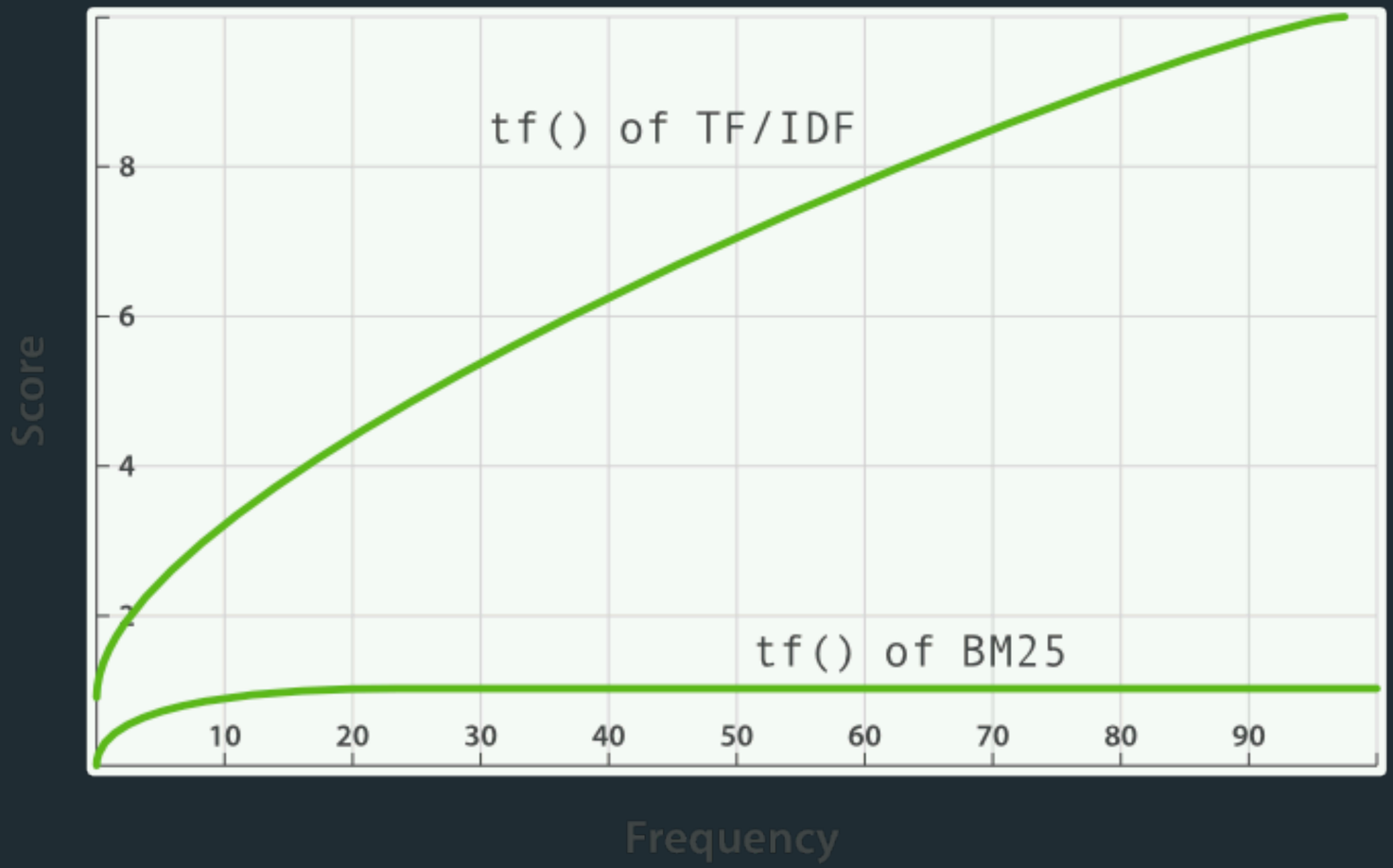
3. ***t.getBoost()*** is a search time boost of term *t* in the query *q* as specified in the query text (see query syntax), or as set by wrapping with `BoostQuery`. Notice that there is really no direct API for accessing a boost of one term in a multi term query, but rather multi terms are represented in a query as multi `TermQuery` objects, and so the boost of a term in the query is accessible by calling the sub-query `getBoost()`.

4. ***norm(t,d)*** is an index-time boost factor that solely depends on the number of tokens of this field in the document, so that shorter fields contribute more to the score.

BM25

- Default in Apache Lucene/Elasticsearch
- Works better with stopwords (high TF)
- Term frequency saturation
- Improved field length normalization (per document)

BM25

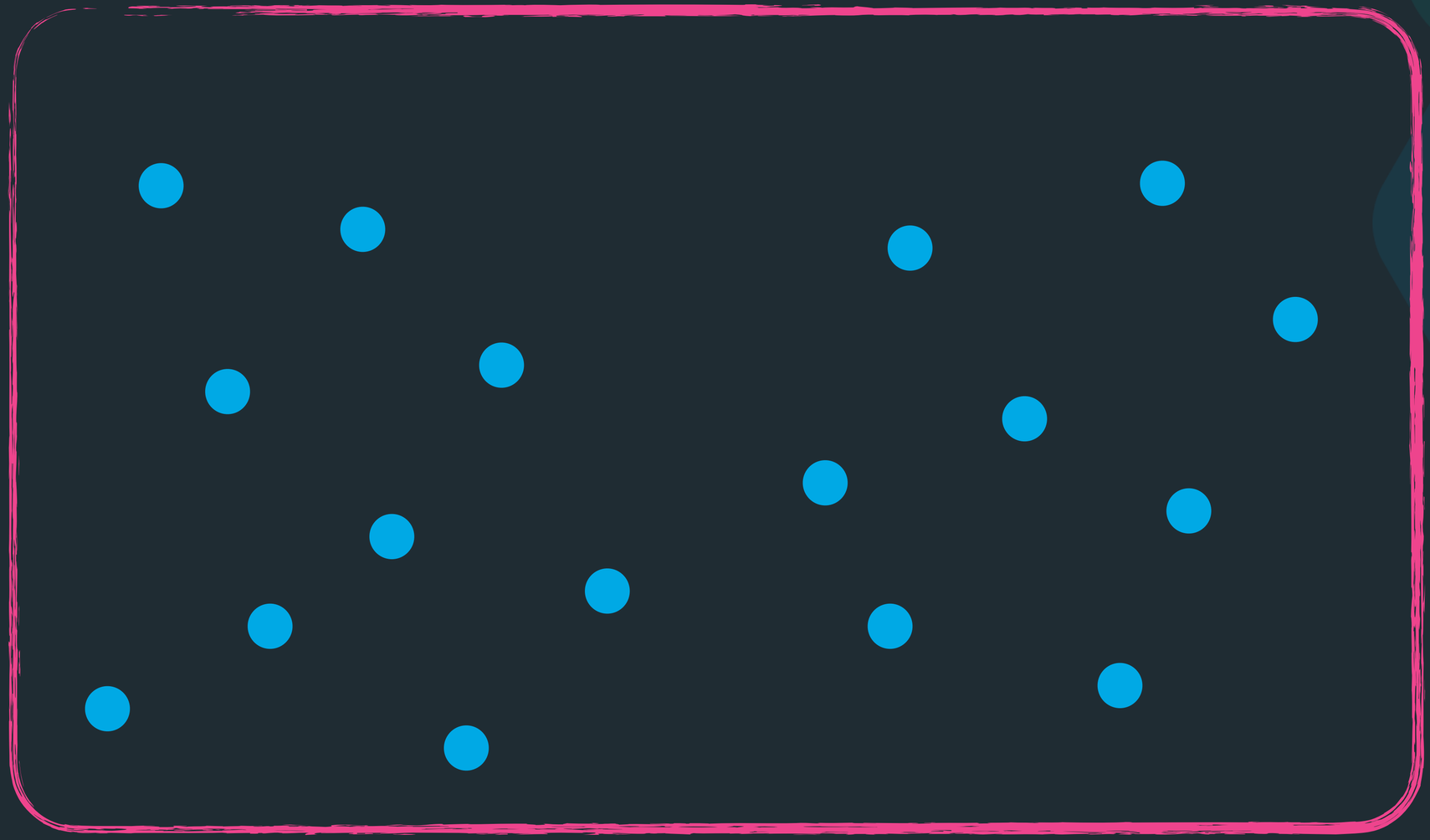


https://www.elastic.co/guide/en/elasticsearch/guide/2.x/pluggable-similarites.html

elastic

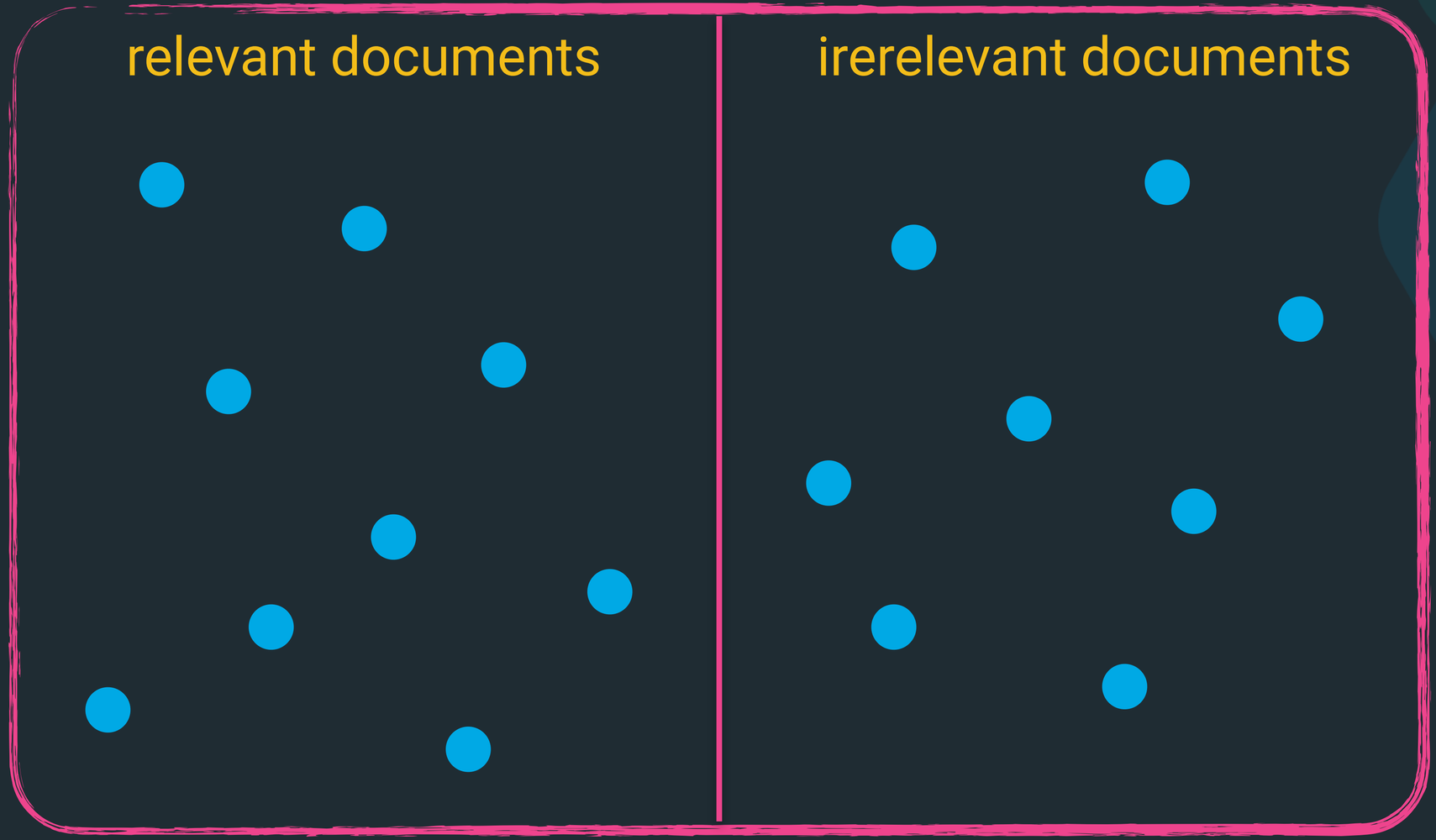
Precision vs. recall

Precision and Recall



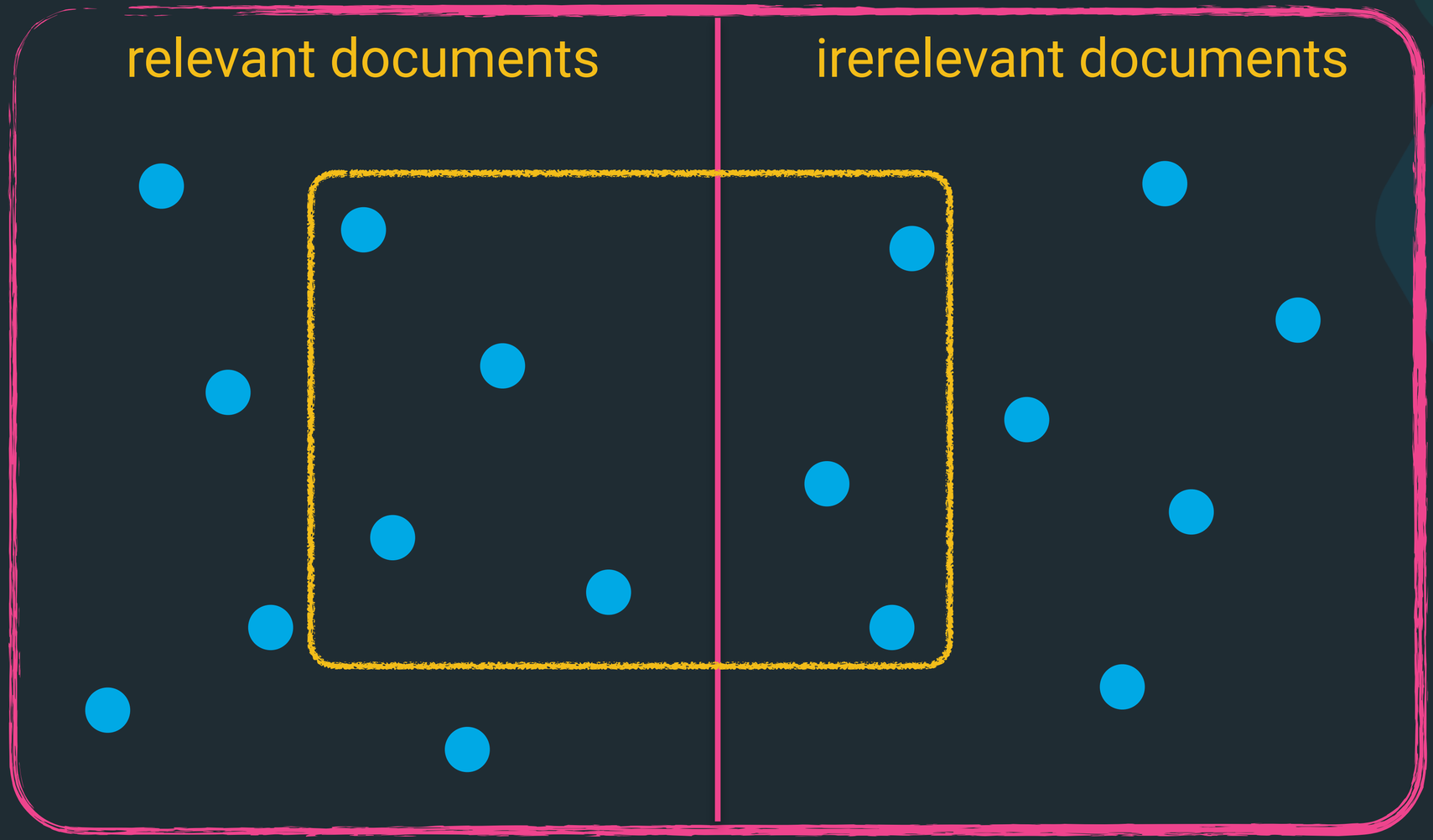
elastic

Precision and Recall



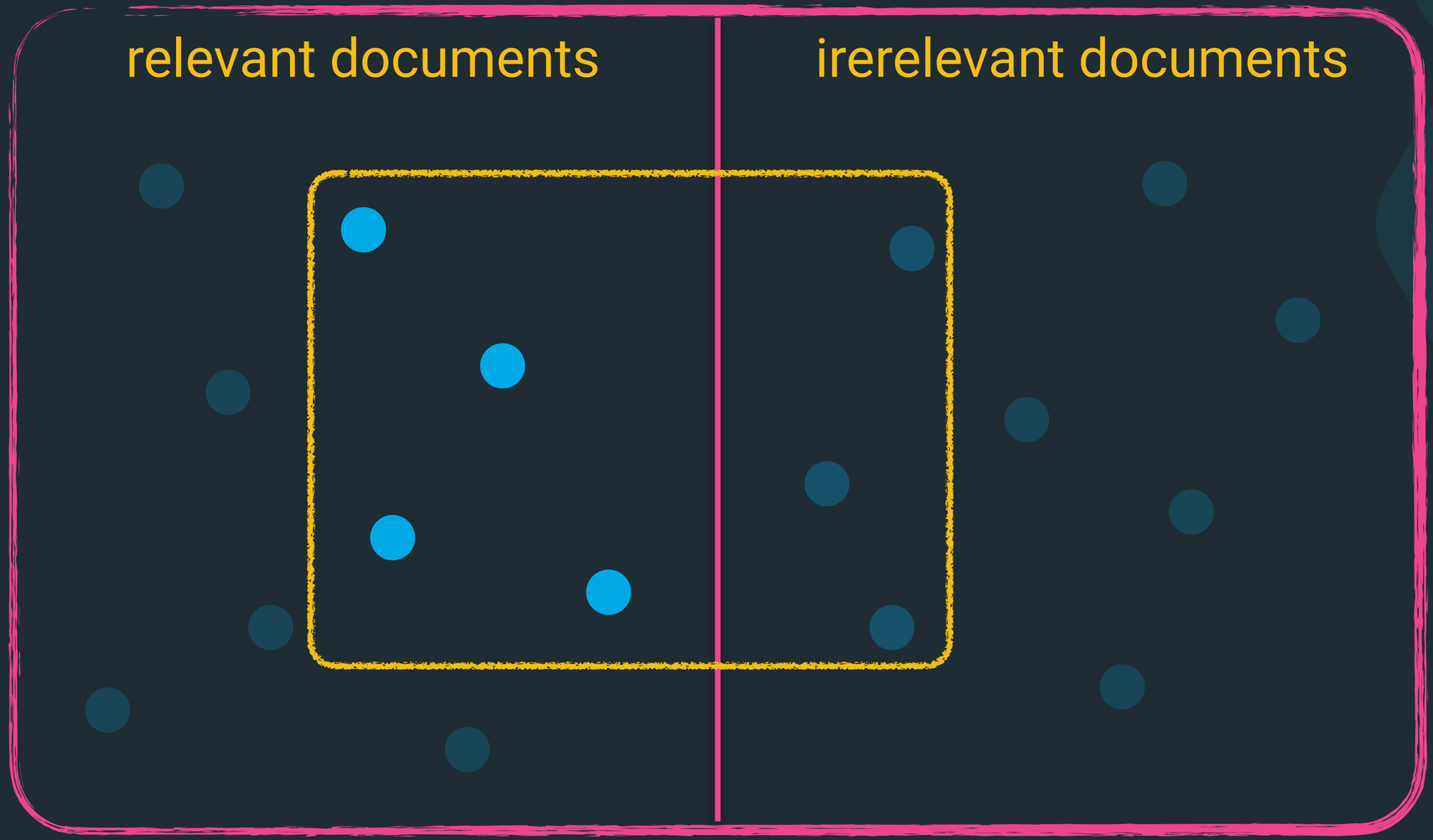
elastic

Precision and Recall



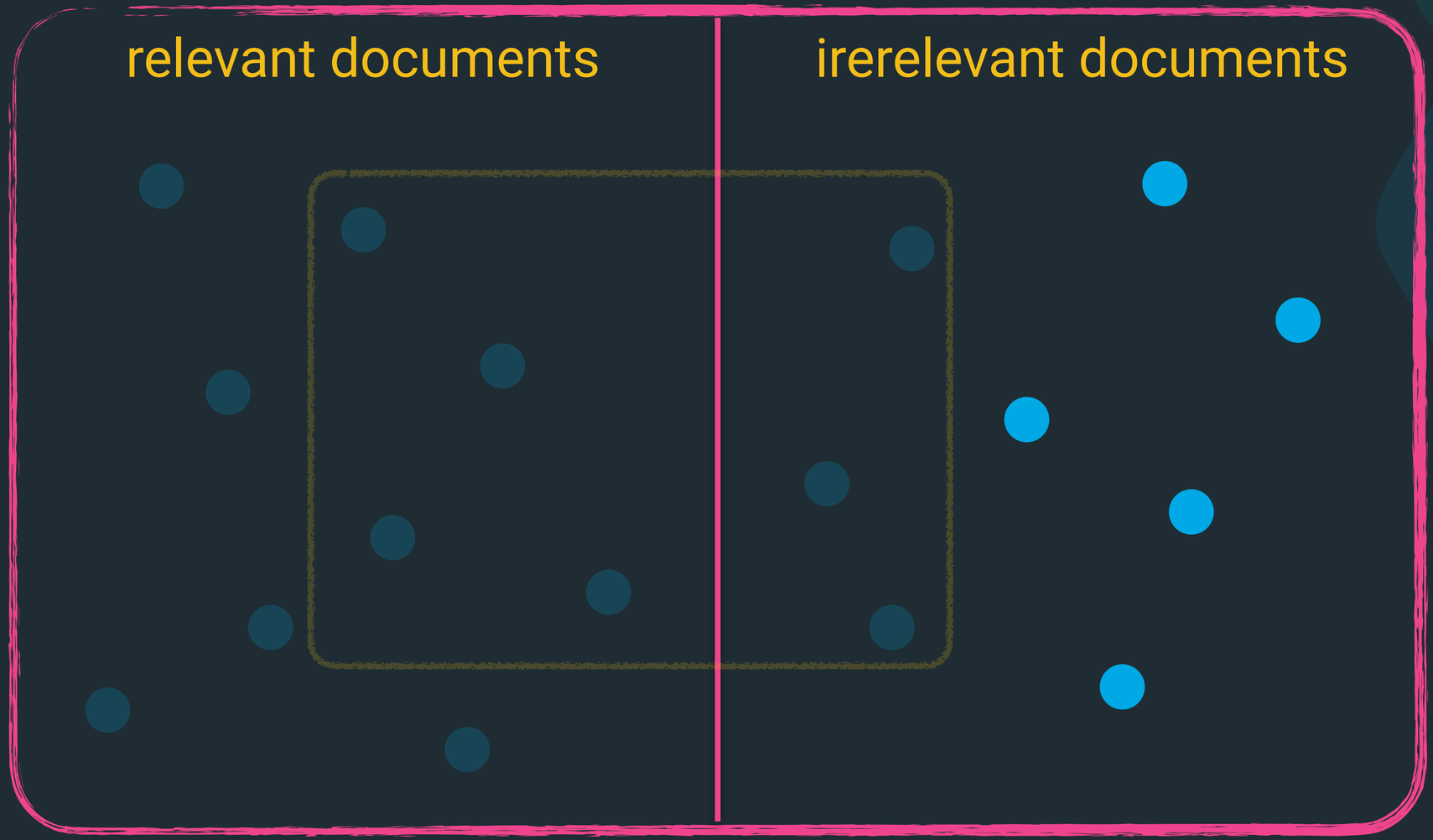
elastic

True positives



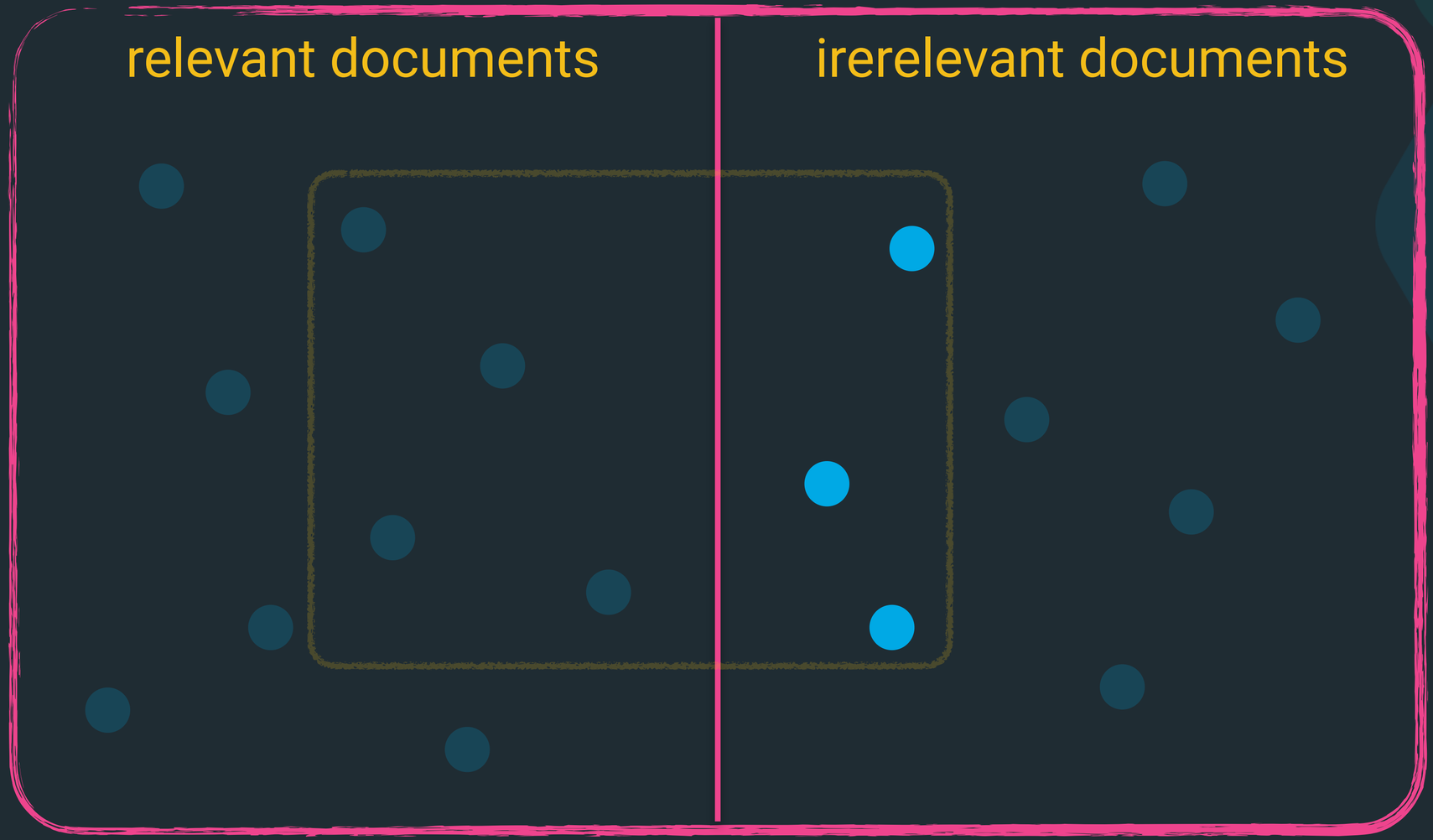
elastic

True negatives



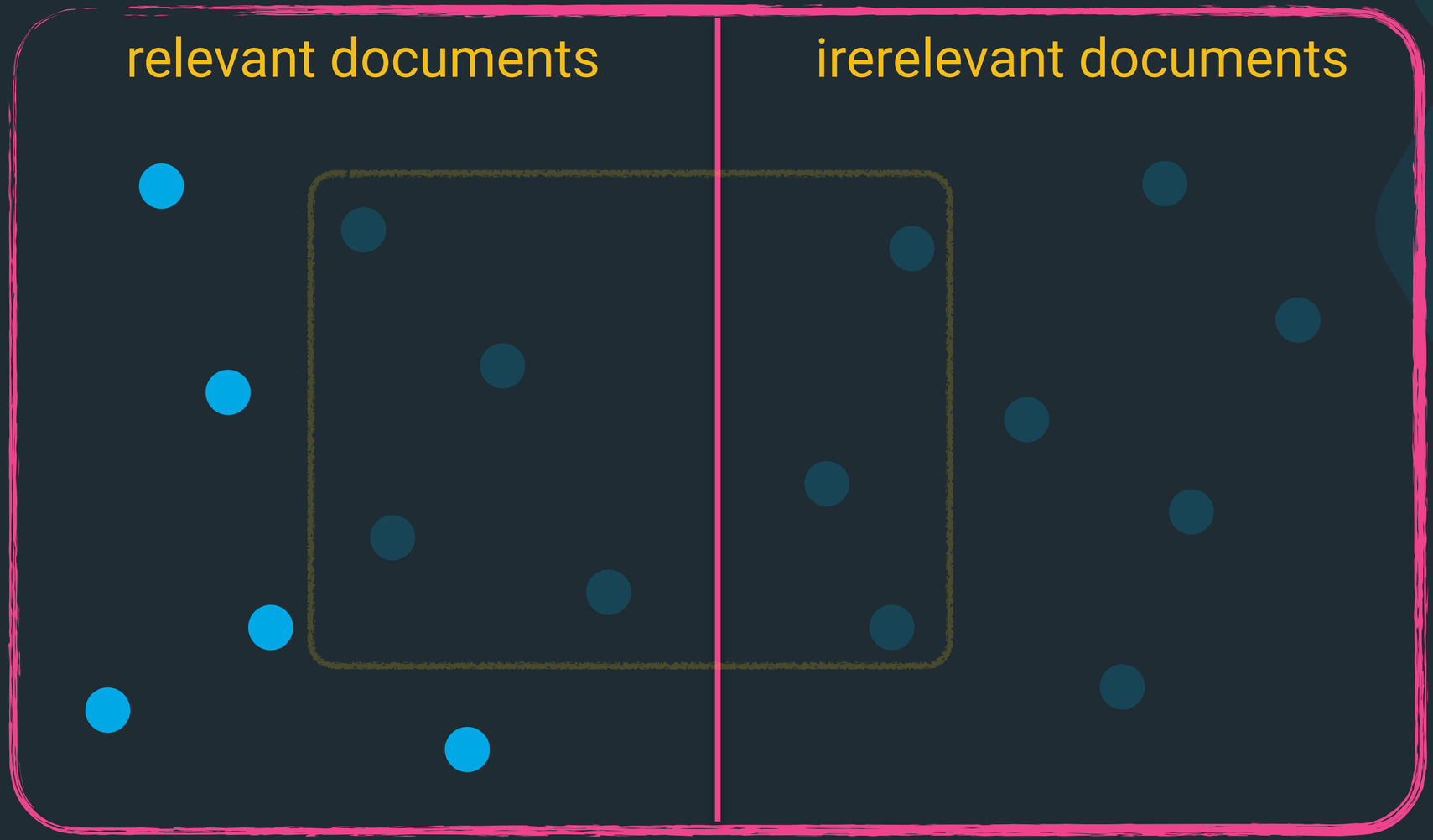
elastic

False positives



elastic

False negatives



elastic

Precision and recall

- Precision: How many selected documents are relevant?
- Recall: How many relevant documents are selected

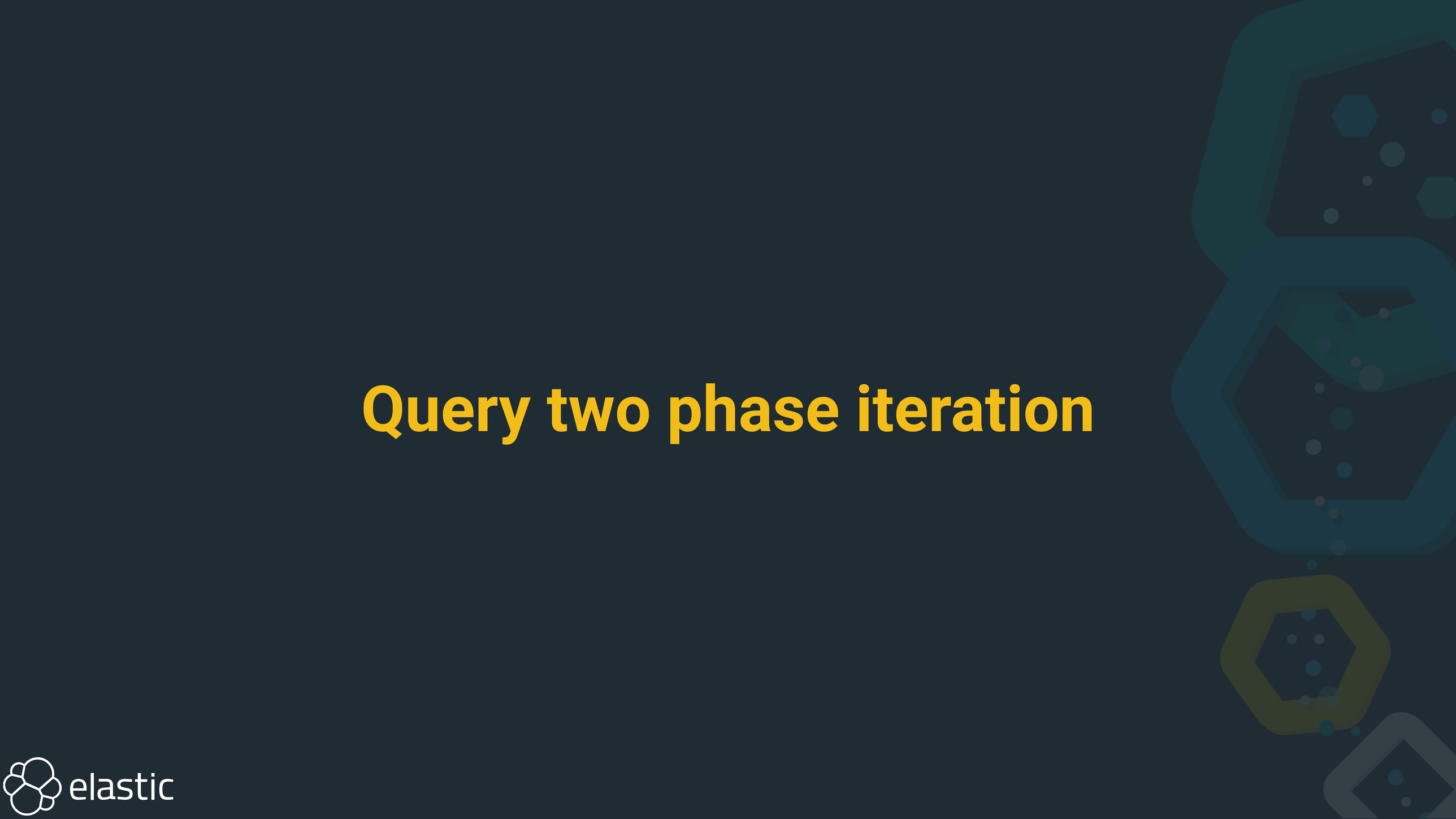
Under the hood

elastic

Optimizations everywhere

- leap frogging, skip lists
- top-k
- two phase iterations
- integer compression

Query two phase iteration



elastic

Two phase iteration: Phrase query

- Phrase query: `"quick fox"`
- Approximation phase: document contains terms `quick` and `fox`
- Verification phase: read positions of terms

Two phase iteration: Geo distance query

- Geo distance query: Distance from reference point
- Approximation phase: bbox around point
- Verification phase: exact distance calculation

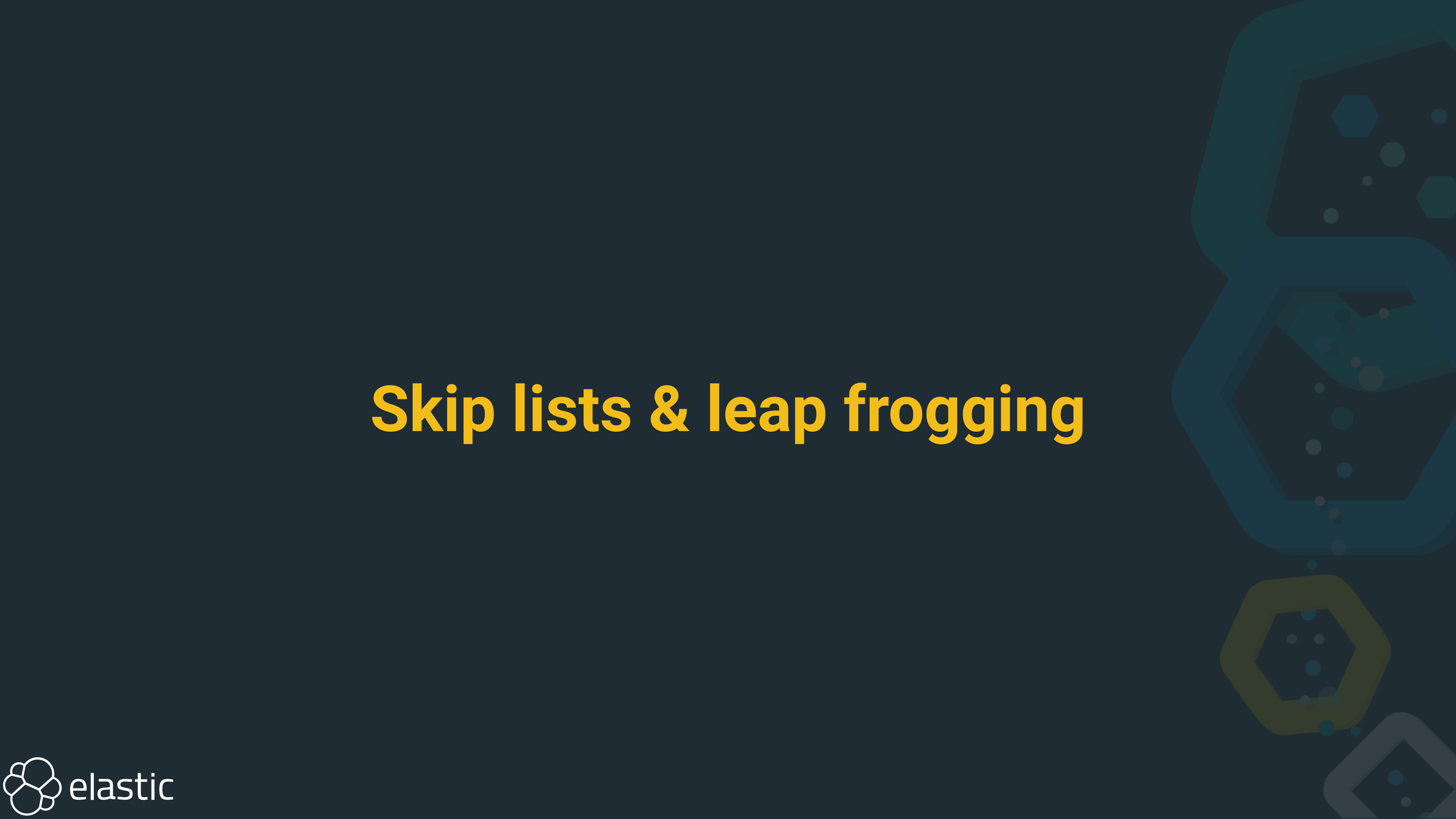
Two phase iteration: Geo distance query

```
GET /my_locations/_search
{
  "query": {
    "bool" : {
      "filter" : {
        "geo_distance" : {
          "distance" : "200km",
          "pin.location" : {
            "lat" : 40,
            "lon" : -70
          }
        }
      }
    }
  }
}
```

Two phase iteration: several queries

- Powerful when several queries are used
- `"quick fox" AND brown`
- Approximation: `quick AND fox AND brown`
- Verification: `"quick fox"` position check for hits

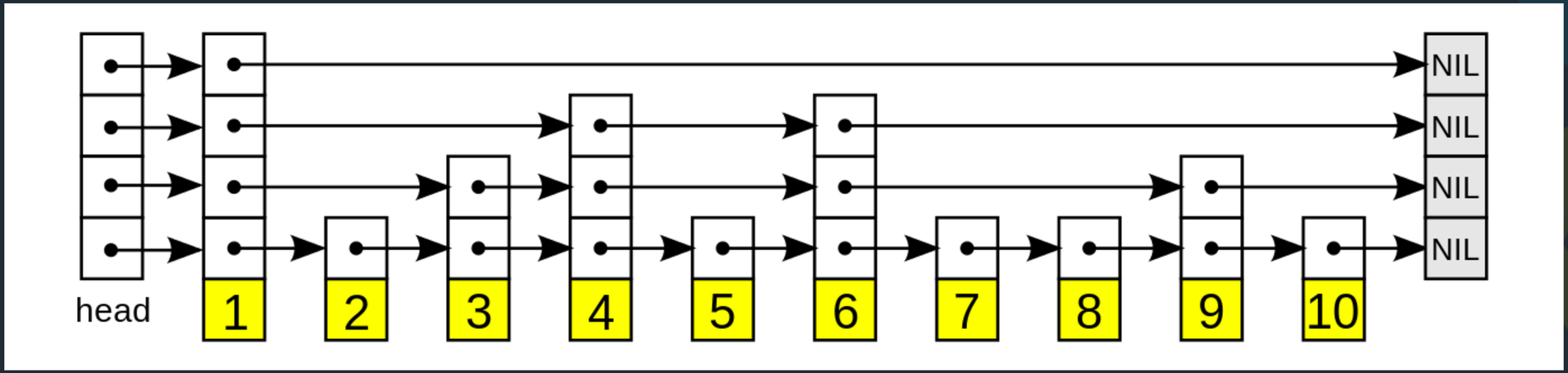
Skip lists & leap frogging



elastic

Skip lists

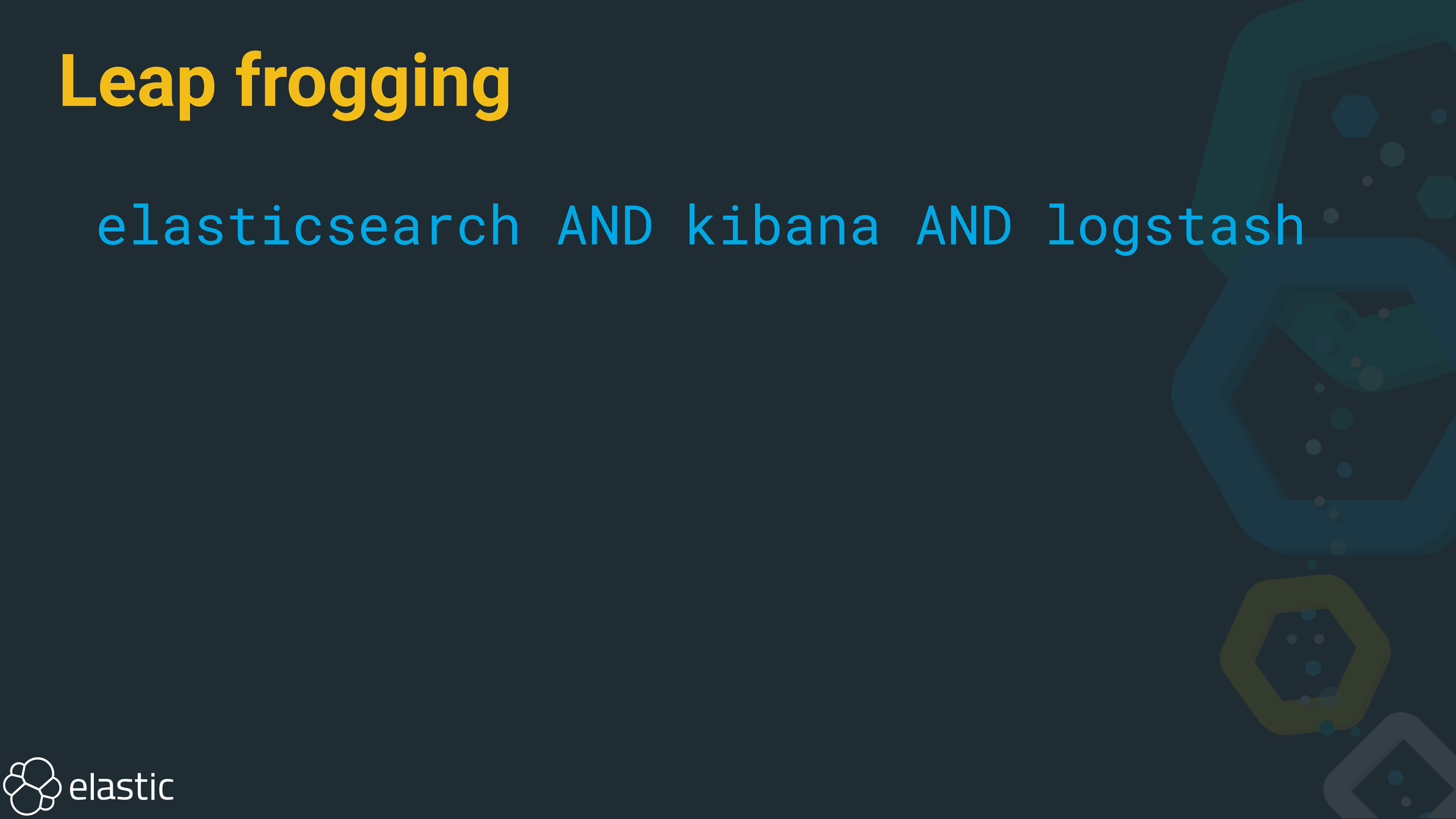
- Term dictionary is a sorted skip list
- Skip list is a linked list with 'express lanes' to leap forward



https://en.wikipedia.org/wiki/Skip_list

Leap frogging

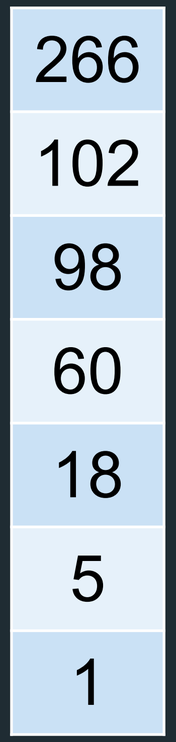
```
elasticsearch AND kibana AND logstash
```

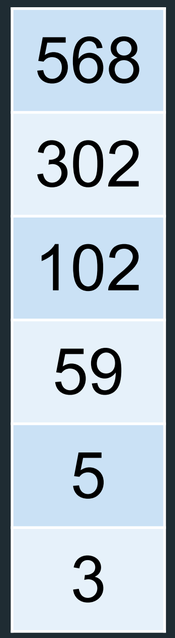


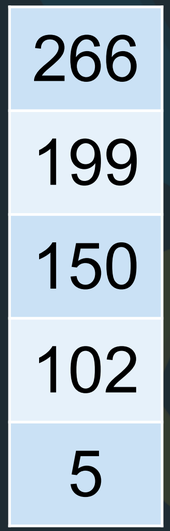
elastic

Leap frogging

```
elasticsearch AND kibana AND logstash
```



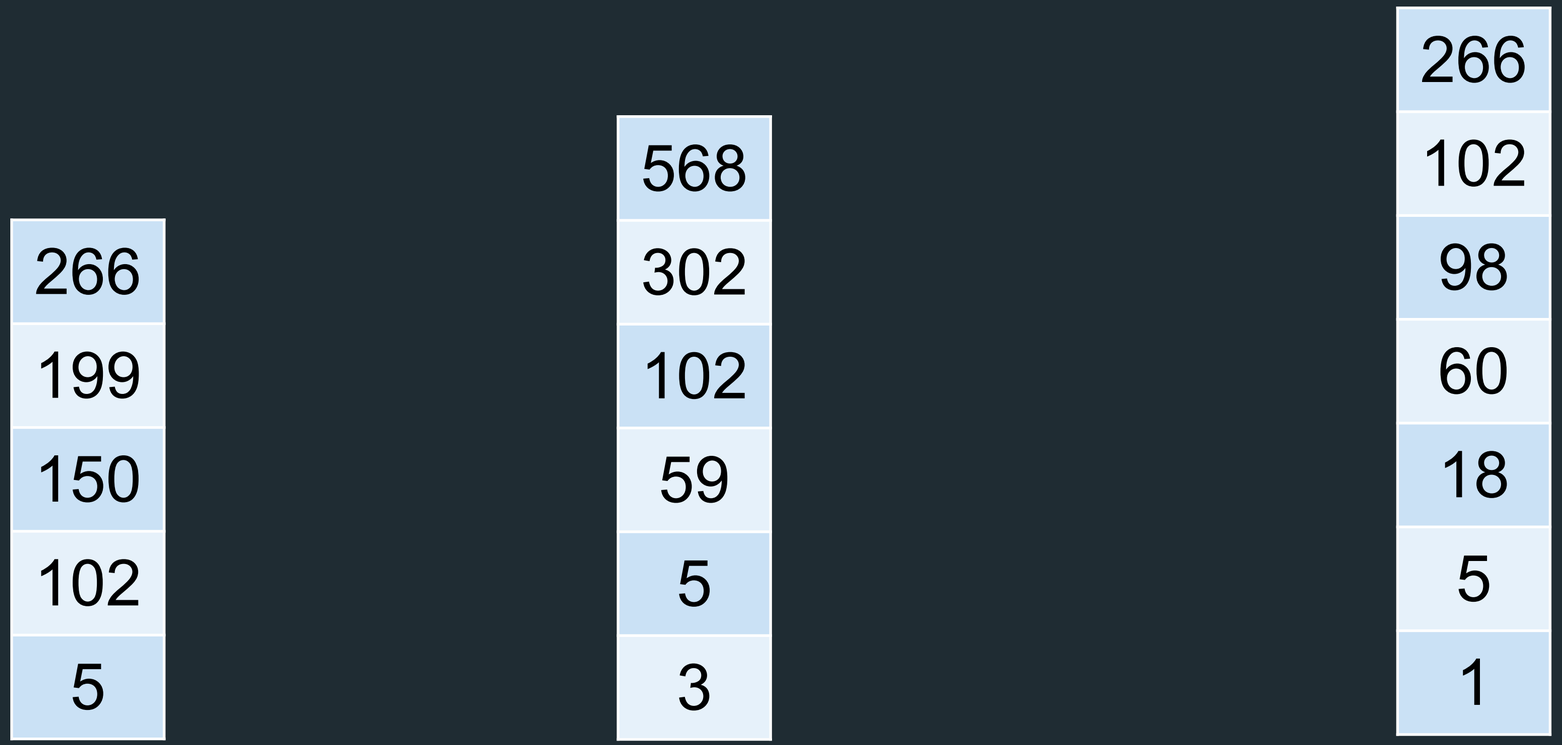




elastic

Leap frogging

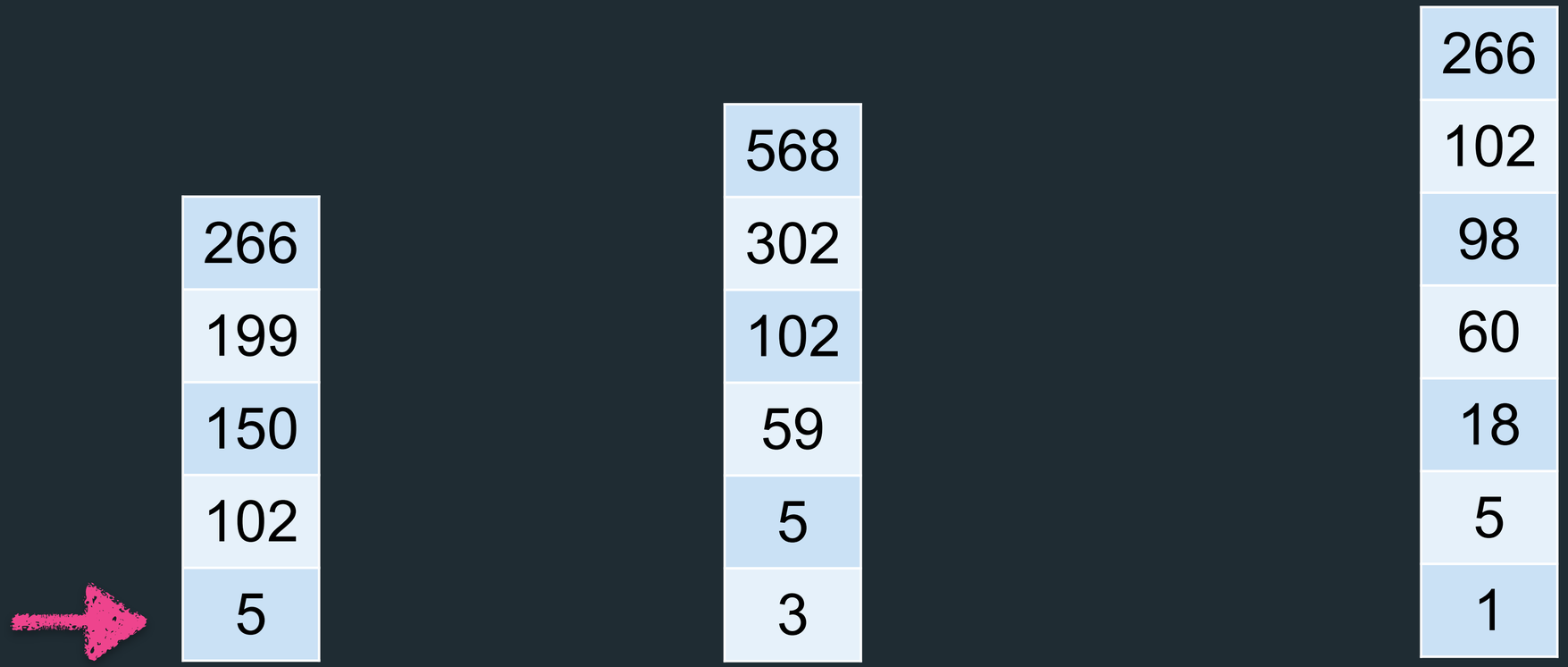
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

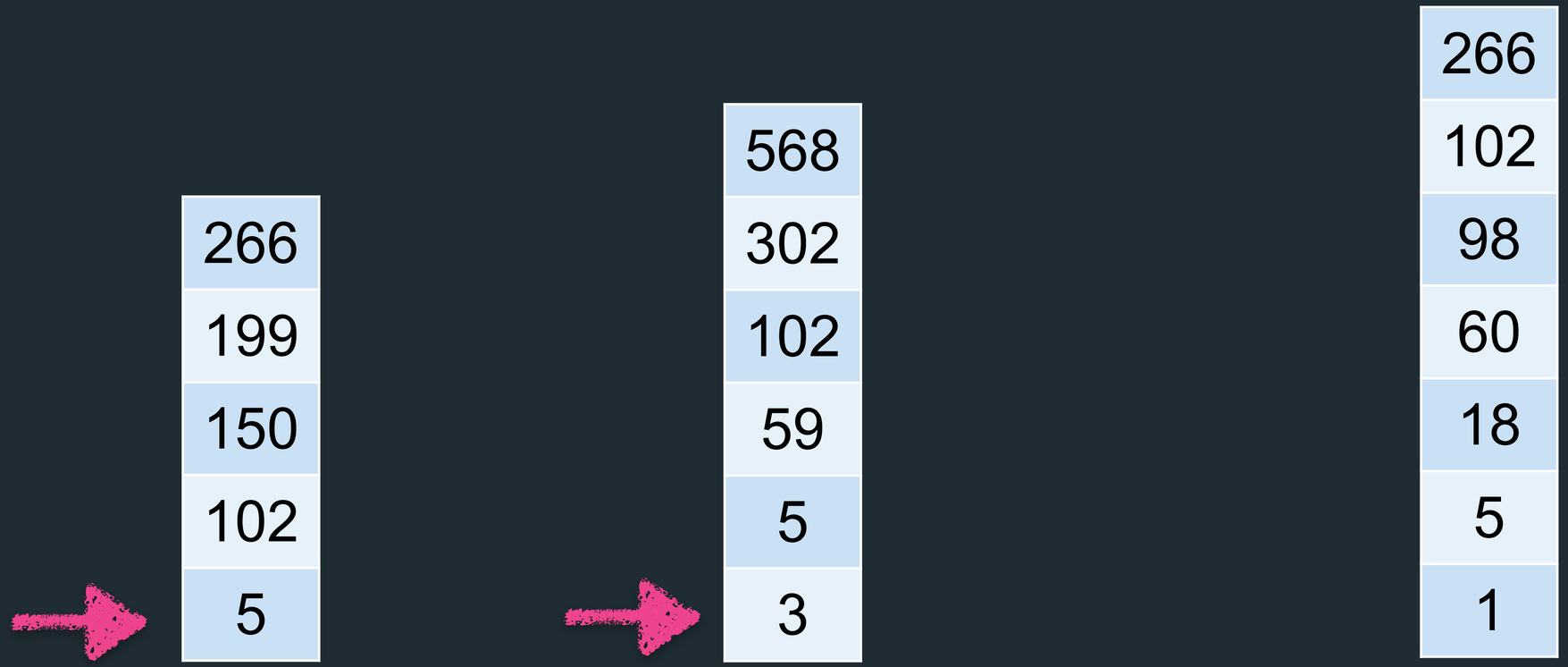
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

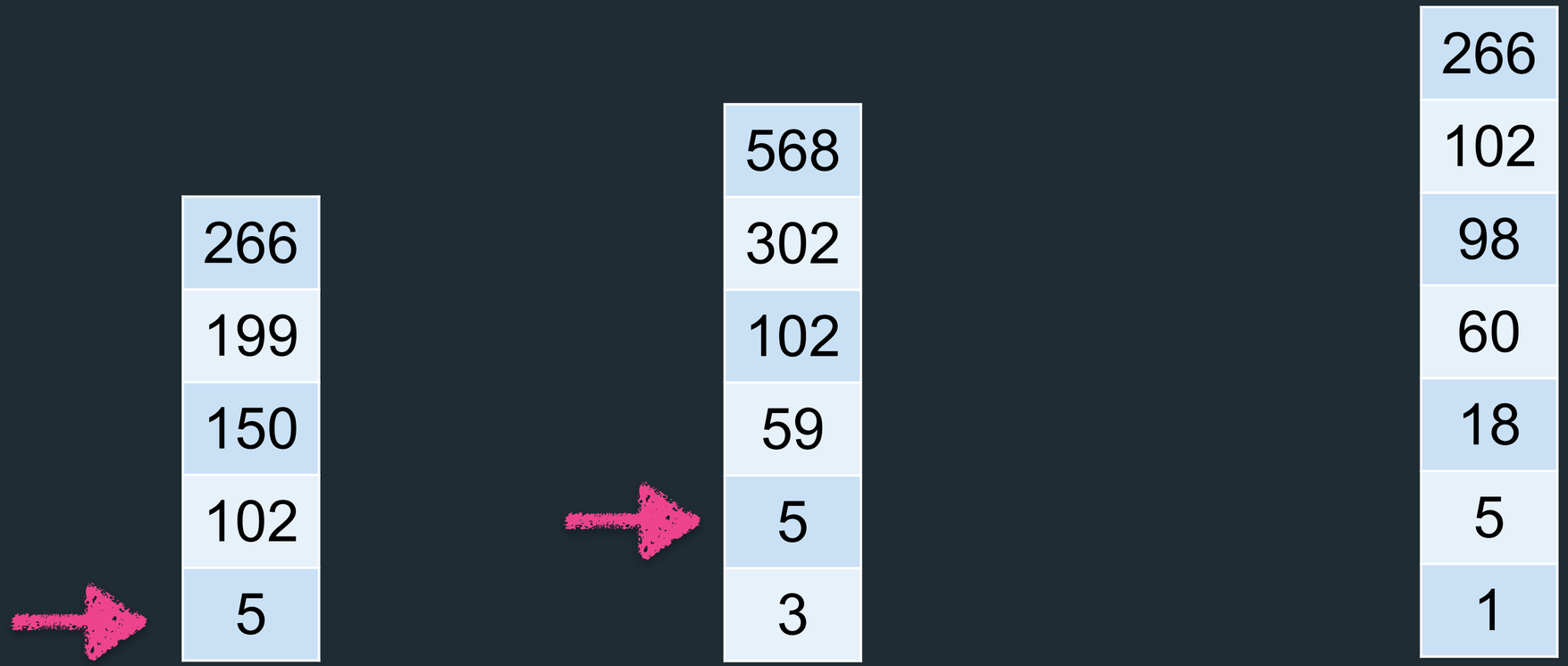
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

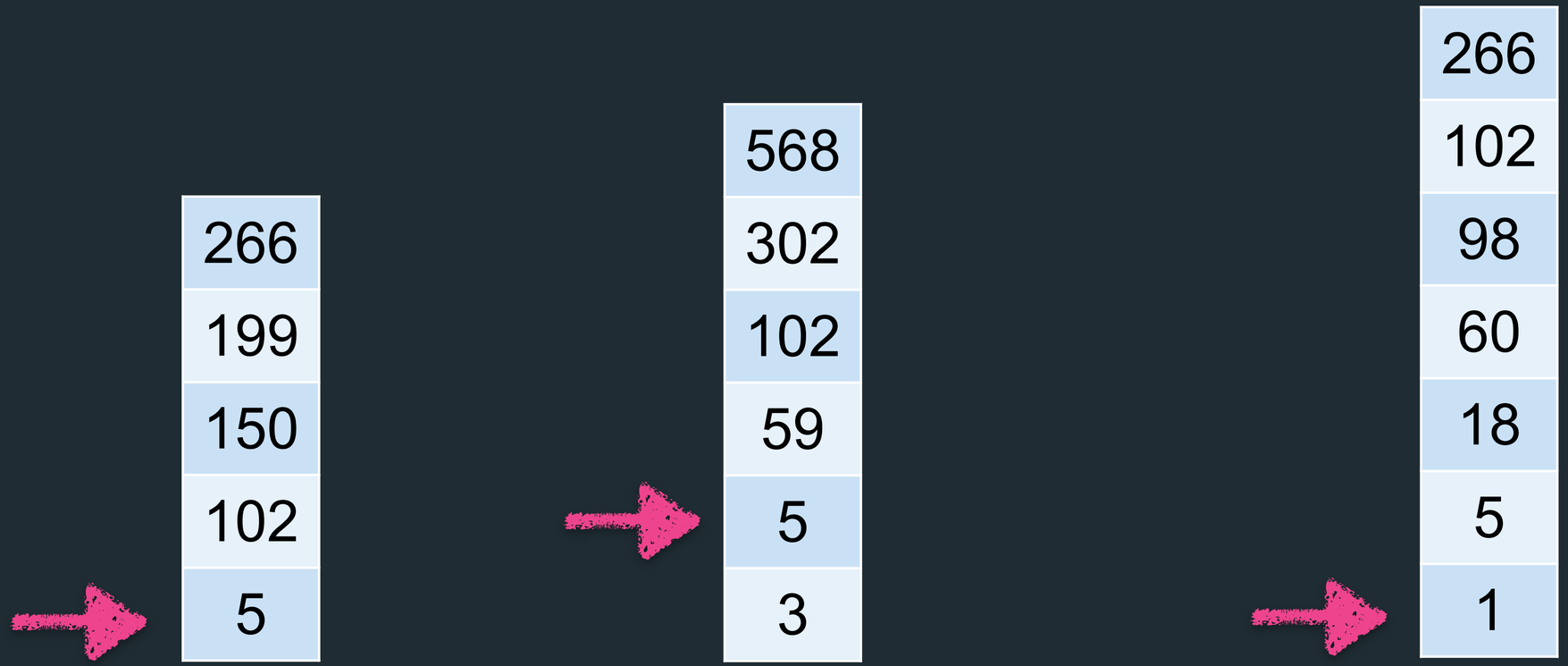
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

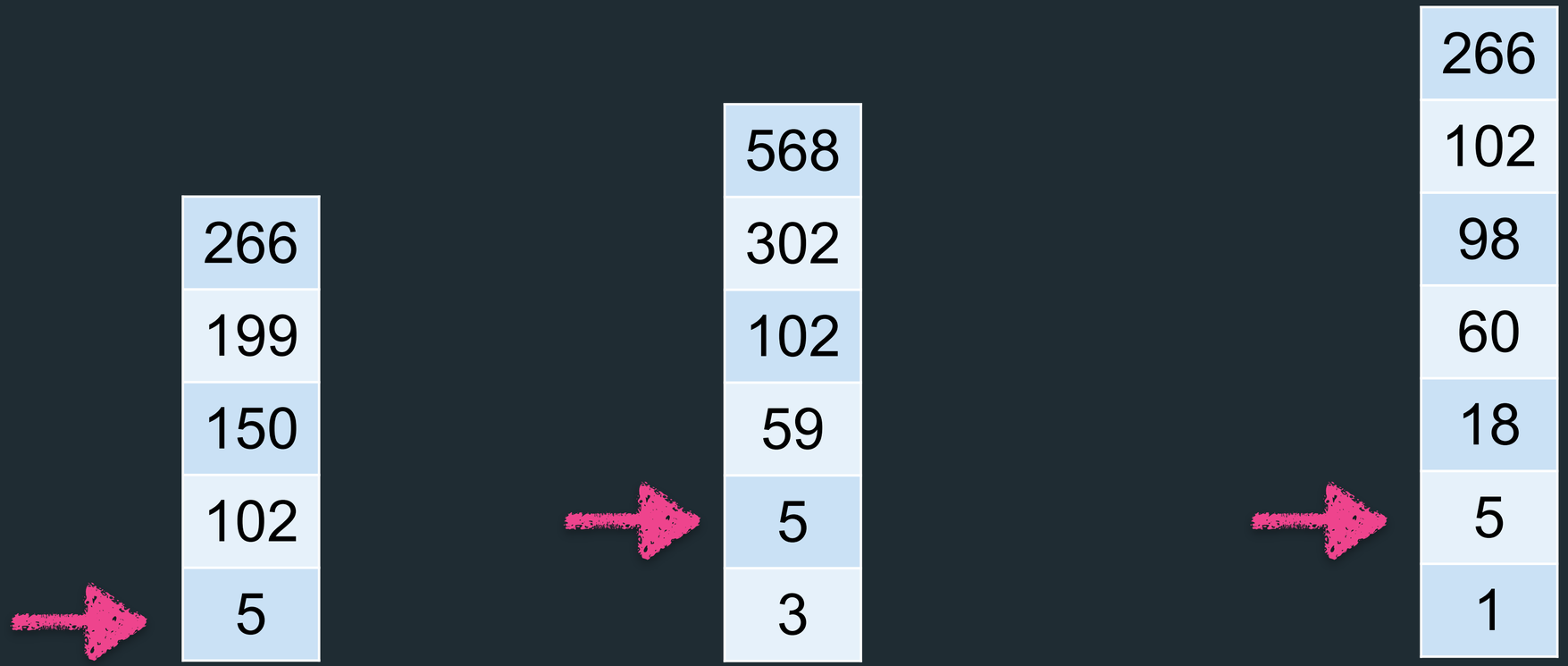
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

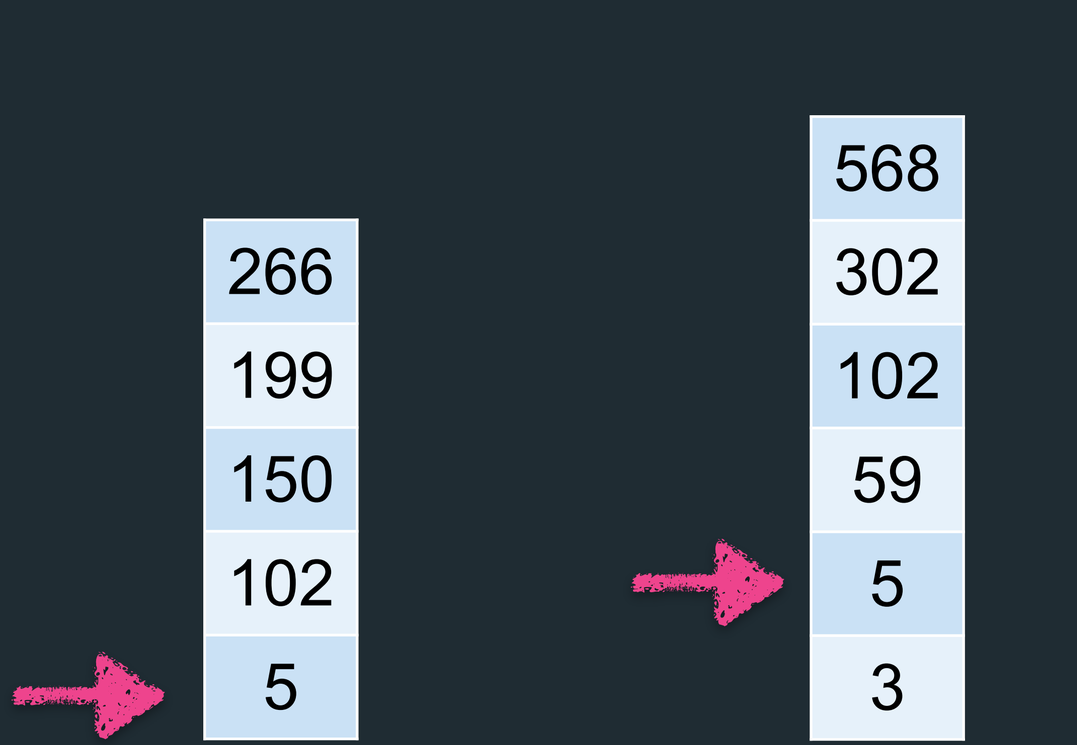
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

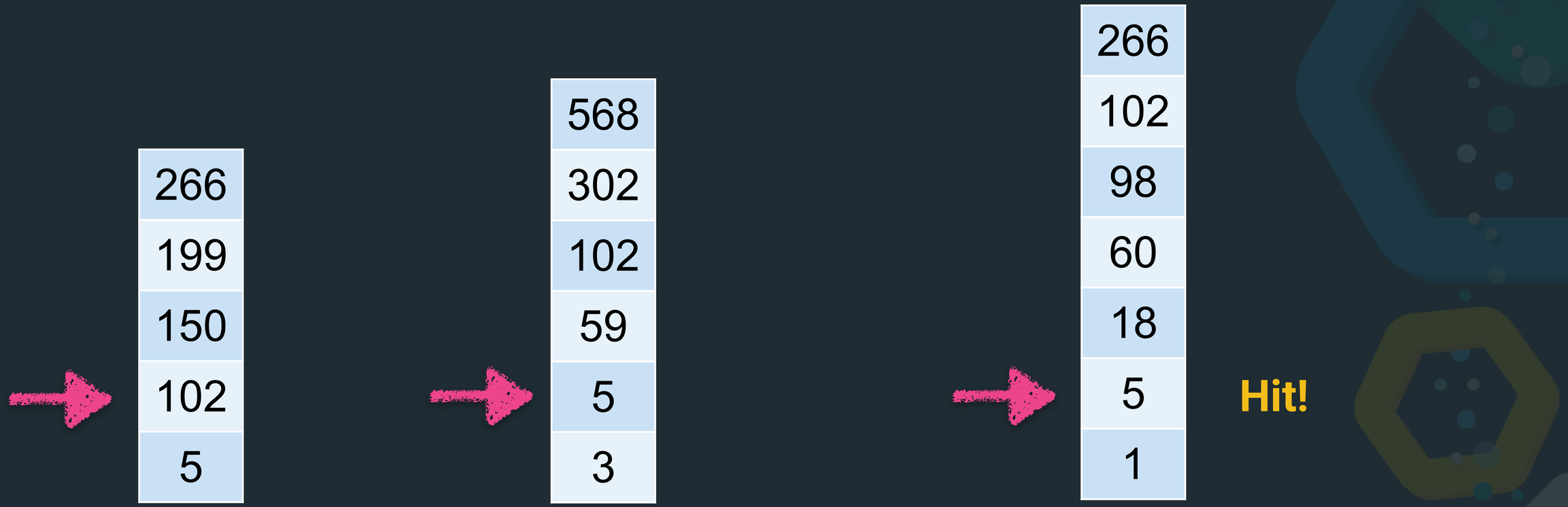
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

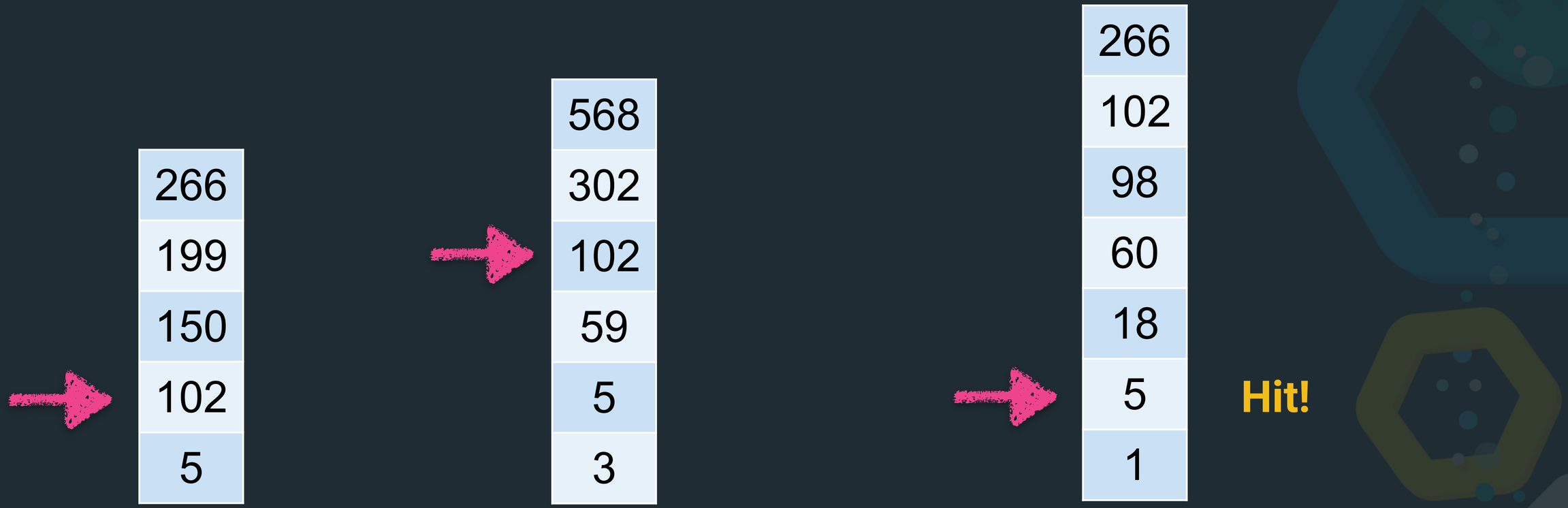
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

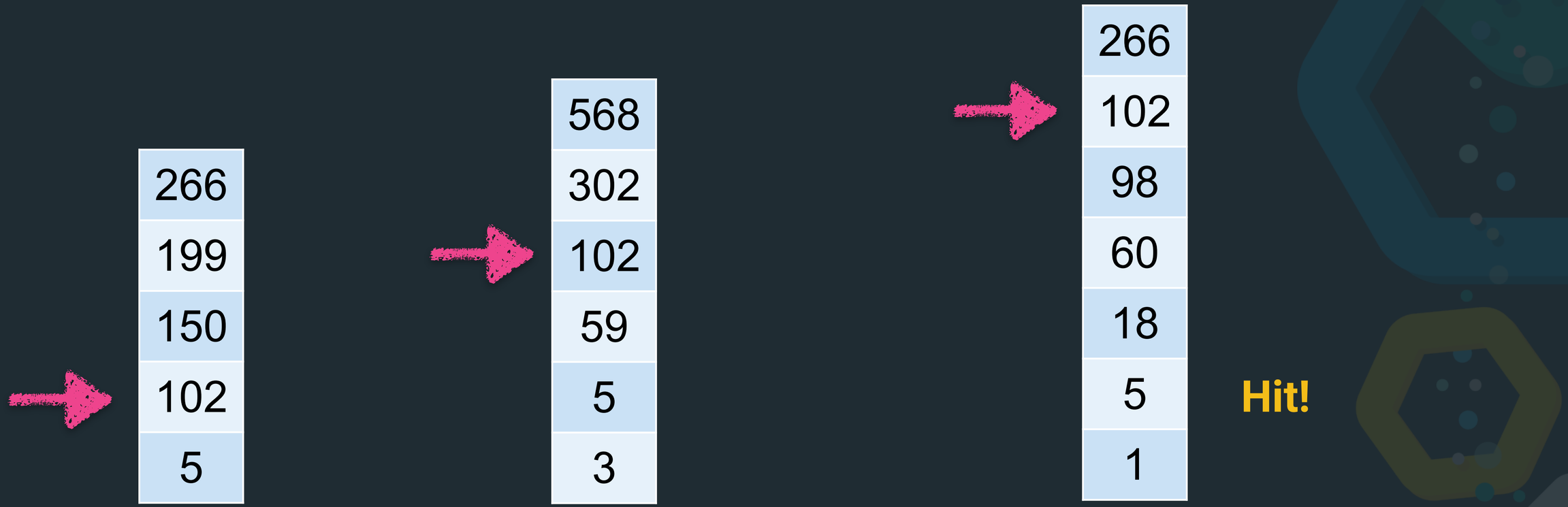
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

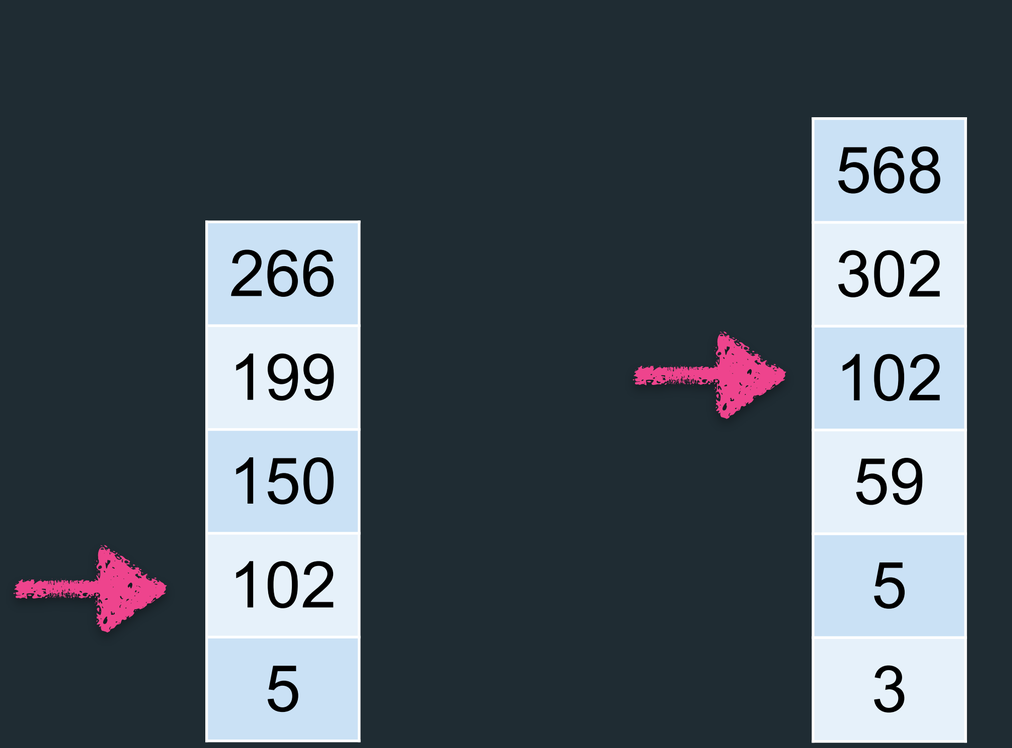
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

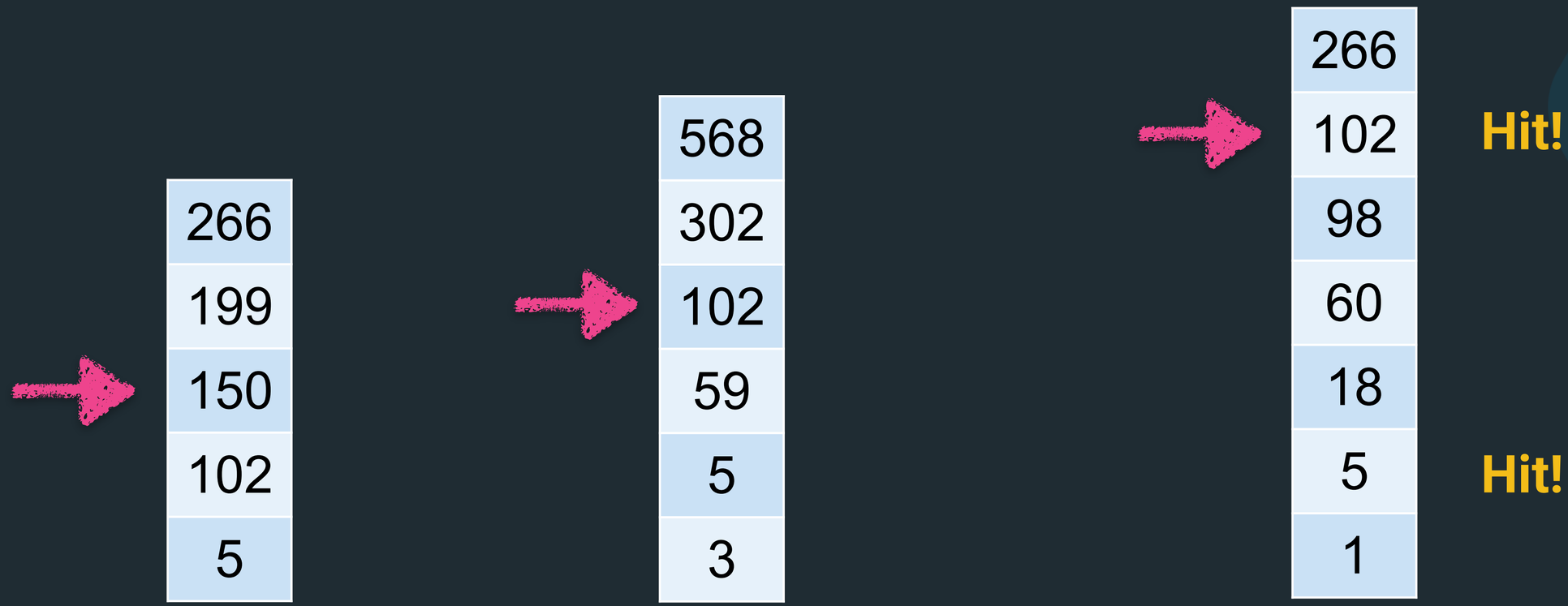
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

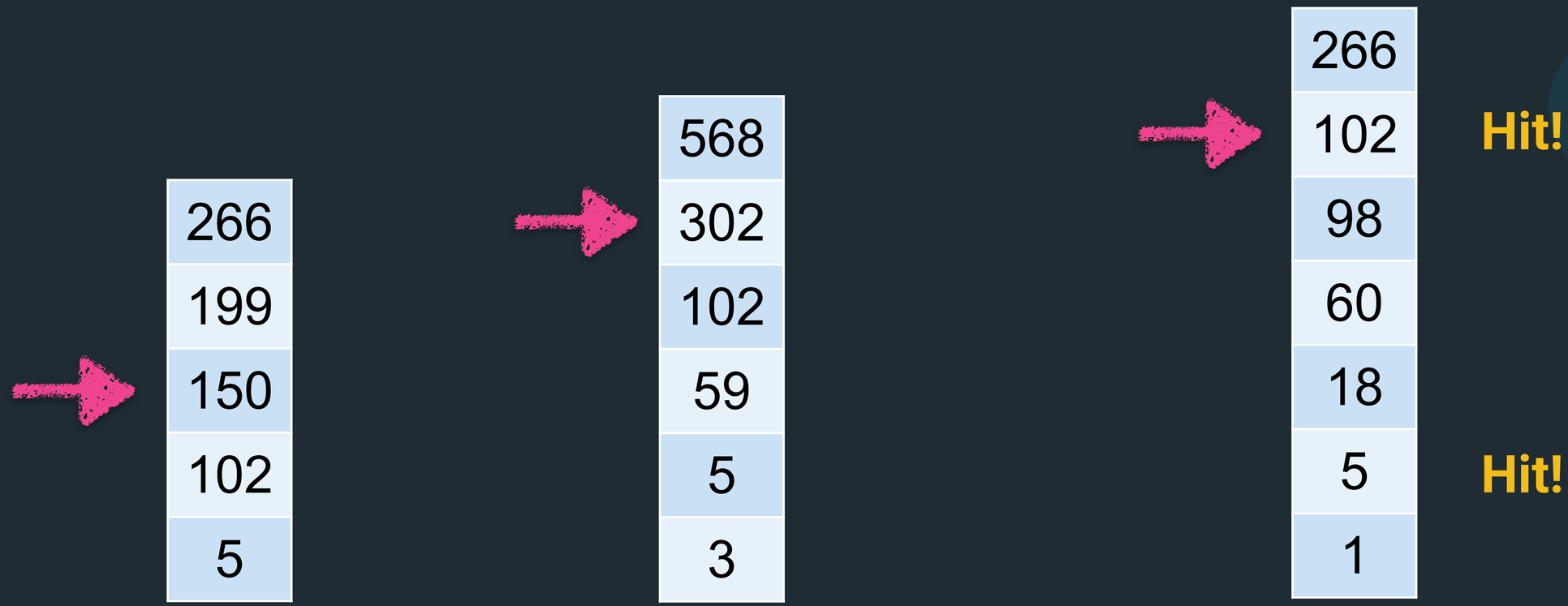
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

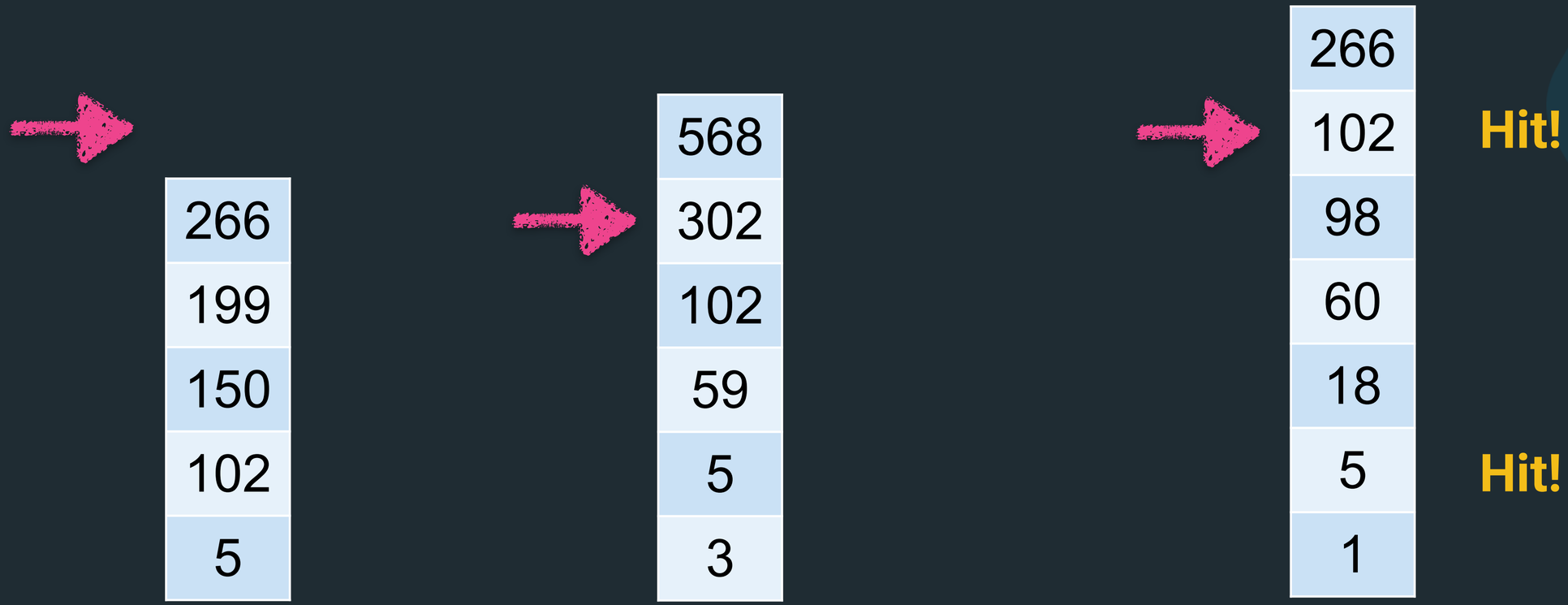
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

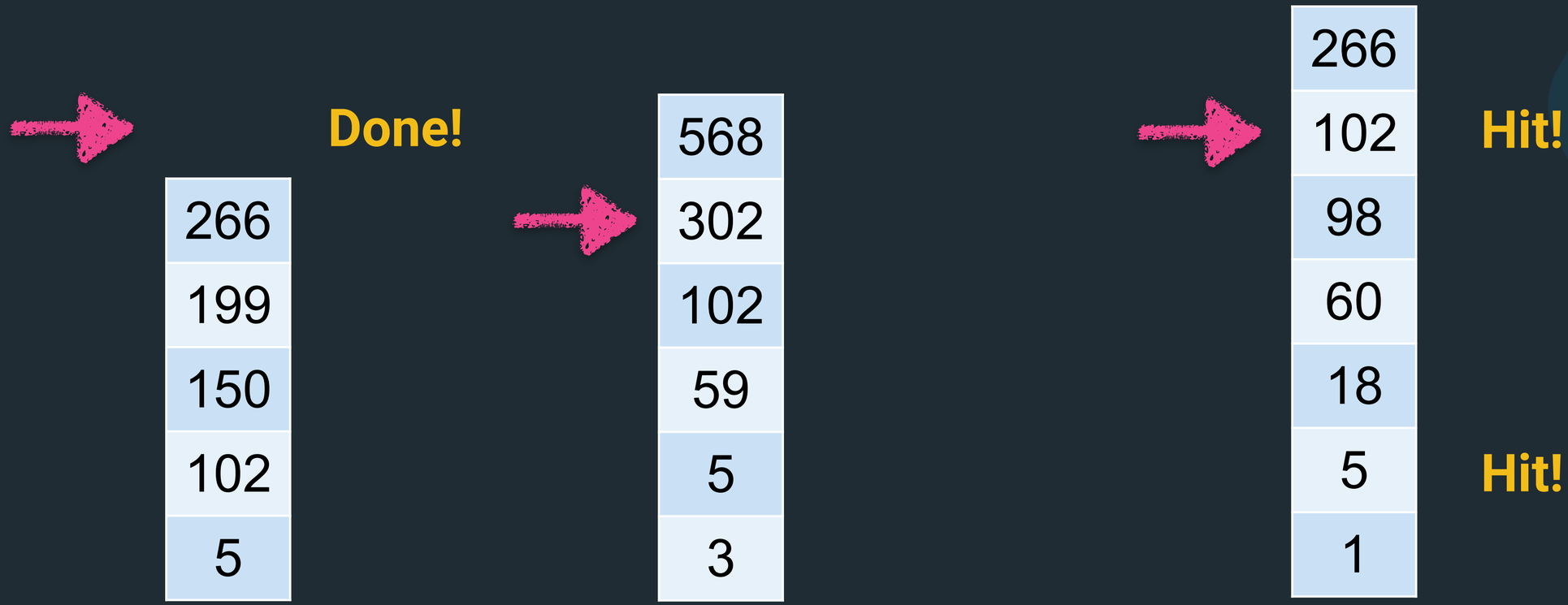
```
logstash AND kibana AND elasticsearch
```



elastic

Leap frogging

```
logstash AND kibana AND elasticsearch
```



elastic

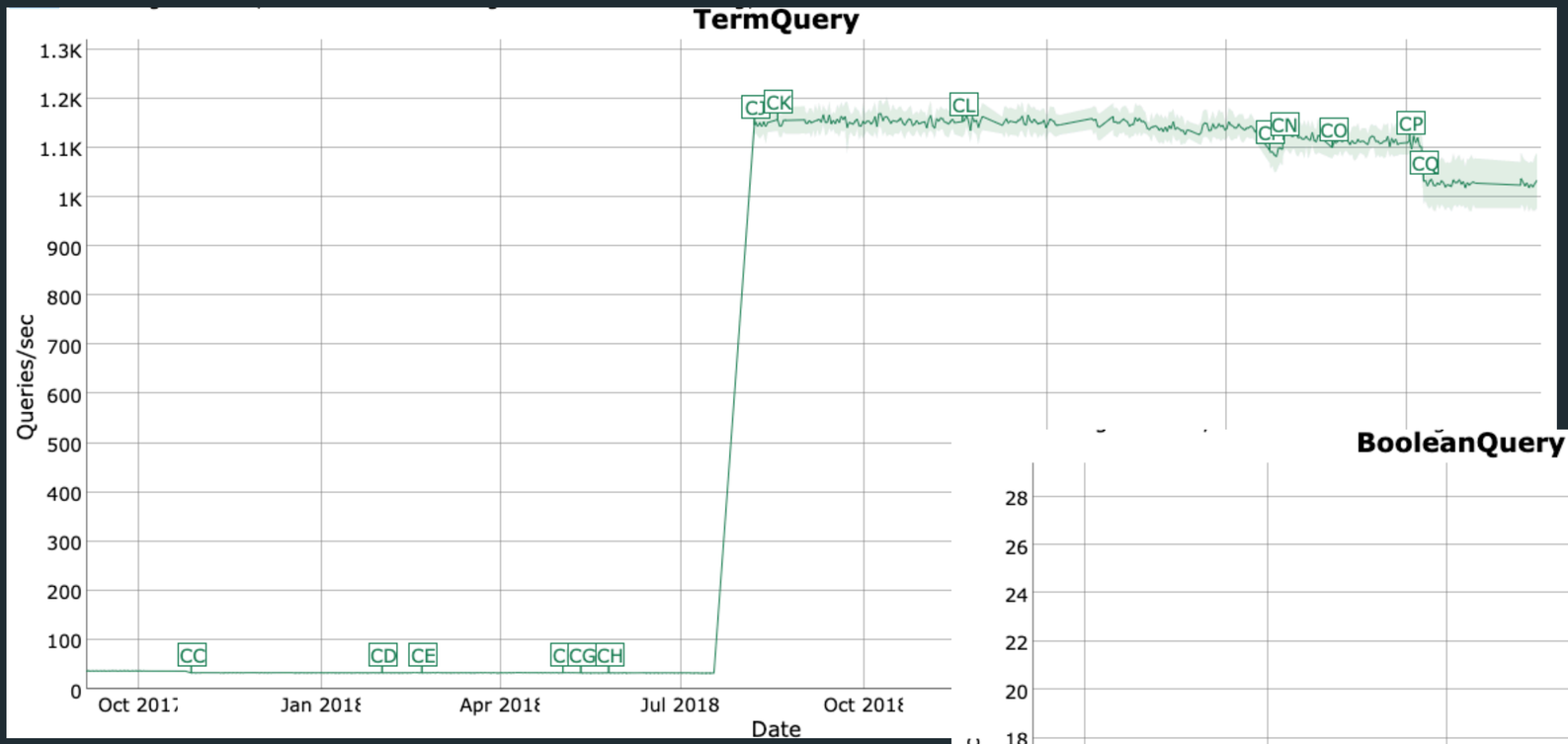
Top-k retrieval

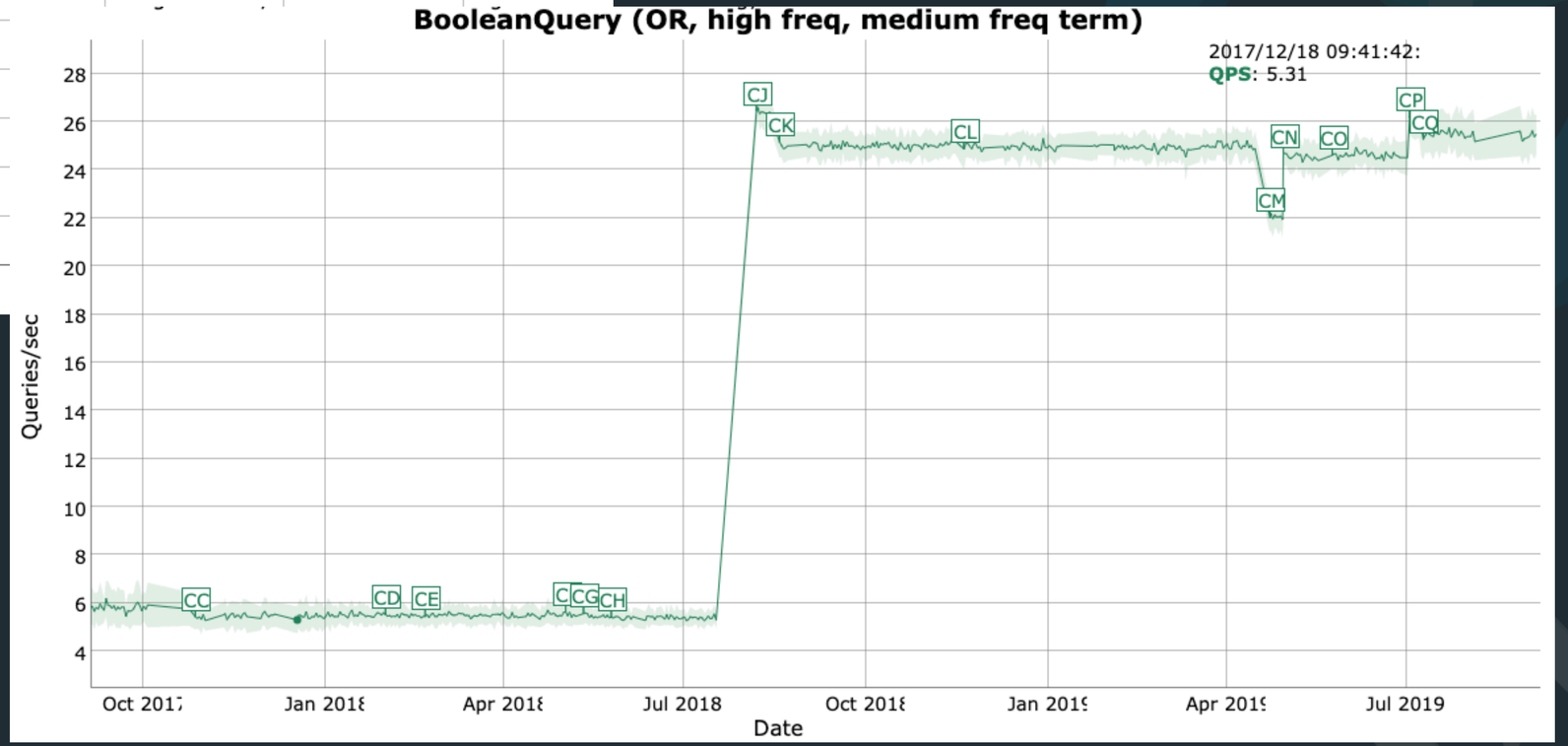
elastic

Top-k retrieval

- `elasticsearch OR kibana`
- top 10 results wanted
- maximum score for `kibana` is 3.0
- maximum score for `elasticsearch` is 5.0
- collecting documents: when 10th hit has score > 3, then only documents with `elasticsearch` need to be collected
- total hit count is not accurate

Top-k retrieval



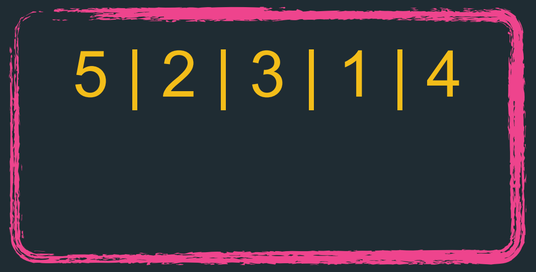


elastic

Index sorting

Order index by field values

- each segment is sorted before write
- criteria can be chosen by the user



retrieve

5 | 2 | 3 | 1 | 4

sort

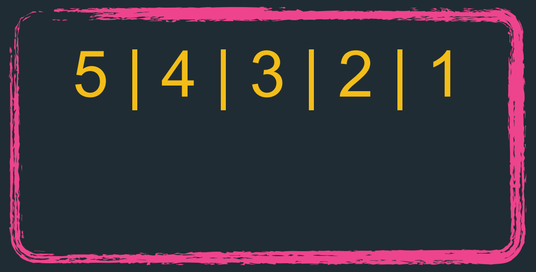
5 | 4 | 3 | 2 | 1

top 2

5 | 4

Order index by field values

- each segment is sorted before write
- criteria can be chosen by the user



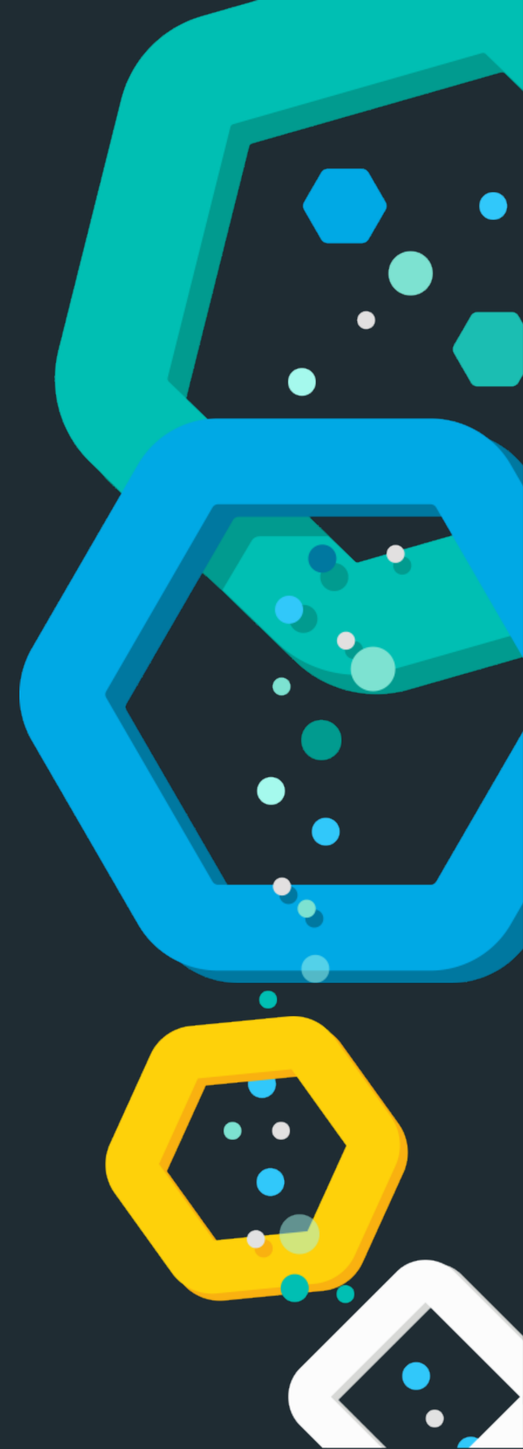
early termination

5 | 4

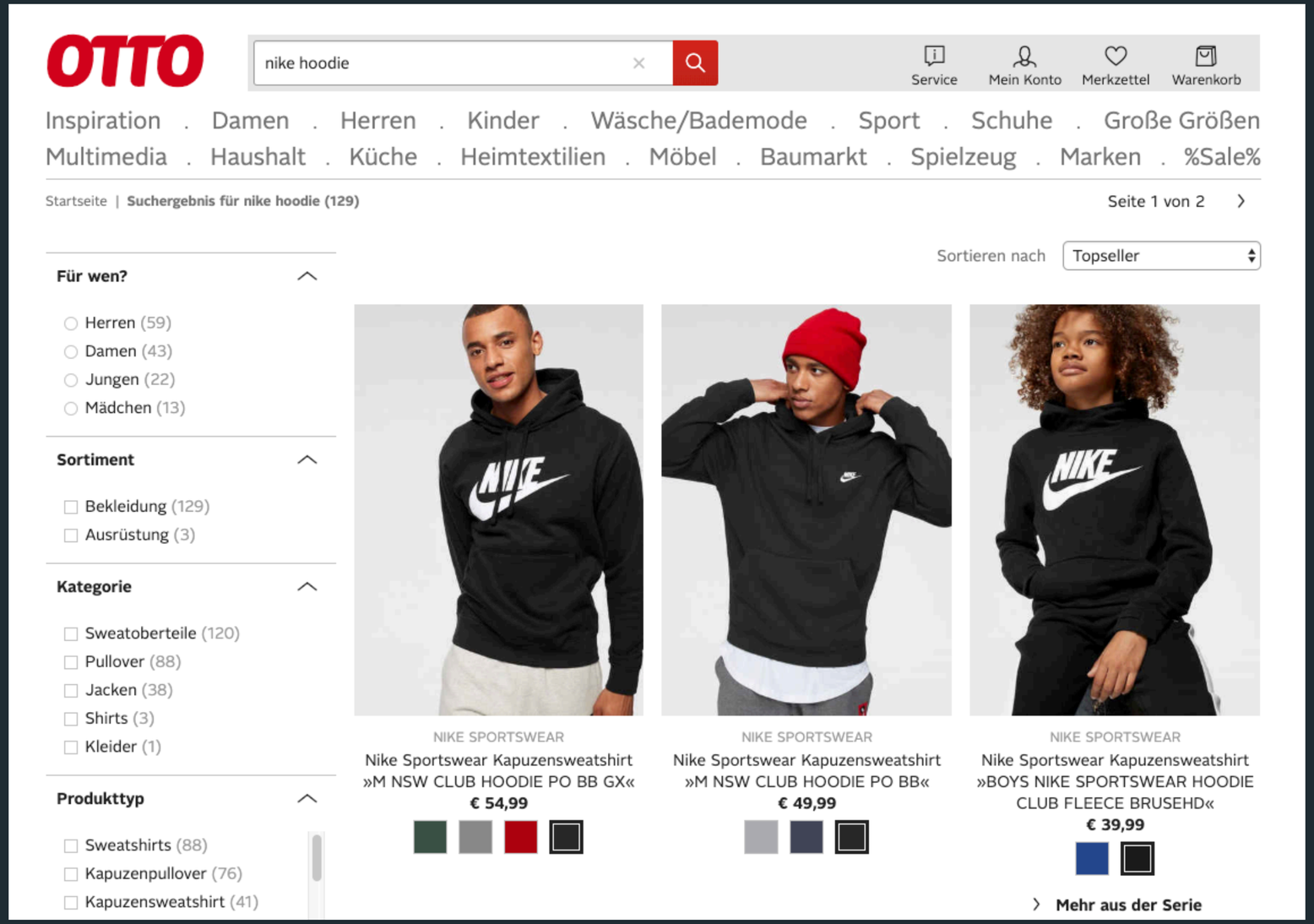
elastic

Aggregations

Reducing data



Aggregations



elastic

OTTO

nike hoodie

Service | Mein Konto | Merkzettel | Warenkorb

Inspiration . Damen . Herren . Kinder . Wäsche/Bademode . Sport . Schuhe . Große Größen
Multimedia . Haushalt . Küche . Heimtextilien . Möbel . Baumarkt . Spielzeug . Marken . %Sale%

Startseite | **Suchergebnis für nike hoodie (129)**

Seite 1 von 2 ›

aggregations

documents

Für wen?

- Herren (59)
- Damen (43)
- Jungen (22)
- Mädchen (13)

Sortiment

- Bekleidung (129)
- Ausrüstung (3)

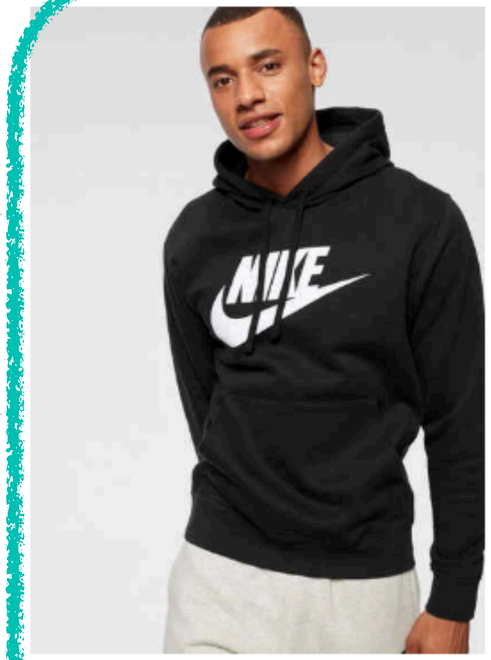
Kategorie

- Sweatoberteile (120)
- Pullover (88)
- Jacken (38)
- Shirts (3)
- Kleider (1)

Produkttyp

- Sweatshirts (88)
- Kapuzenpullover (76)
- Kapuzensweatshirt (4…)

Sortieren nach Topseller



NIKE SPORTSWEAR
Nike Sportswear Kapuzensweatshirt »M NSW CLUB HOODIE PO BB GX«
€ 54,99

NIKE SPORTSWEAR
Nike Sportswear Kapuzensweatshirt »M NSW CLUB HOODIE PO BB«
€ 49,99

NIKE SPORTSWEAR
Nike Sportswear Kapuzensweatshirt »BOYS NIKE SPORTSWEAR HOODIE CLUB FLEECE BRUSEHD«
€ 39,99

› **Mehr aus der Serie**

elast

OTTO

nike hoodie

Service | Mein Konto | Merkzettel | Warenkorb

Inspiration . Damen . Herren . Kinder . Wäsche/Bademode . Sport . Schuhe . Große Größen
Multimedia . Haushalt . Küche . Heimtextilien . Möbel . Baumarkt . Spielzeug . Marken . %Sale%

Startseite | **Suchergebnis für nike hoodie (129)**

Seite 1 von 2 ›

aggregations

documents

Für wen?

- Herren (59)
- Damen (43)
- Jungen (22)
- Mädchen (13)

Sortiment

- Bekleidung (129)
- Ausrüstung (3)

Kategorie

- Sweatoberteile (120)
- Pullover (88)
- Jacken (38)
- Shirts (3)
- Kleider (1)

Produkttyp

- Sweatshirts (88)
- Kapuzenpullover (76)
- Kapuzensweatshirt (41)

Sortieren nach Topseller

NIKE SPORTSWEAR

Nike Sportswear Kapuzensweatshirt »M NSW CLUB HOODIE PO BB GX«

€ 54,99

NIKE SPORTSWEAR

Nike Sportswear Kapuzensweatshirt »M NSW CLUB HOODIE PO BB«

€ 49,99

NIKE SPORTSWEAR

Nike Sportswear Kapuzensweatshirt »BOYS NIKE SPORTSWEAR HOODIE CLUB FLEECE BRUSEHD«

€ 39,99

› **Mehr aus der Serie**

elast

Bucketing documents

Pumps

Sneakers

Oxfords

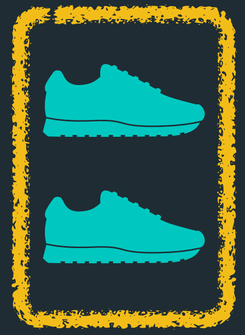
Sneakers

Boots

elastic

Bucketing documents

Sneakers



Pumps

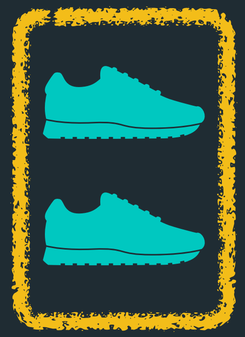
Boots

Oxfords

elastic

Bucketing documents

Sneakers



2

Pumps

1

Boots

1

Oxfords

1

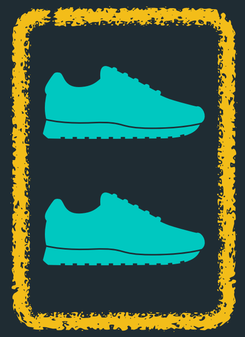
bucket agg

metric agg

doc_count

Bucketing documents

Sneakers



50

Pumps

95

Boots

90

Oxfords

23

bucket agg

metric agg

avg price

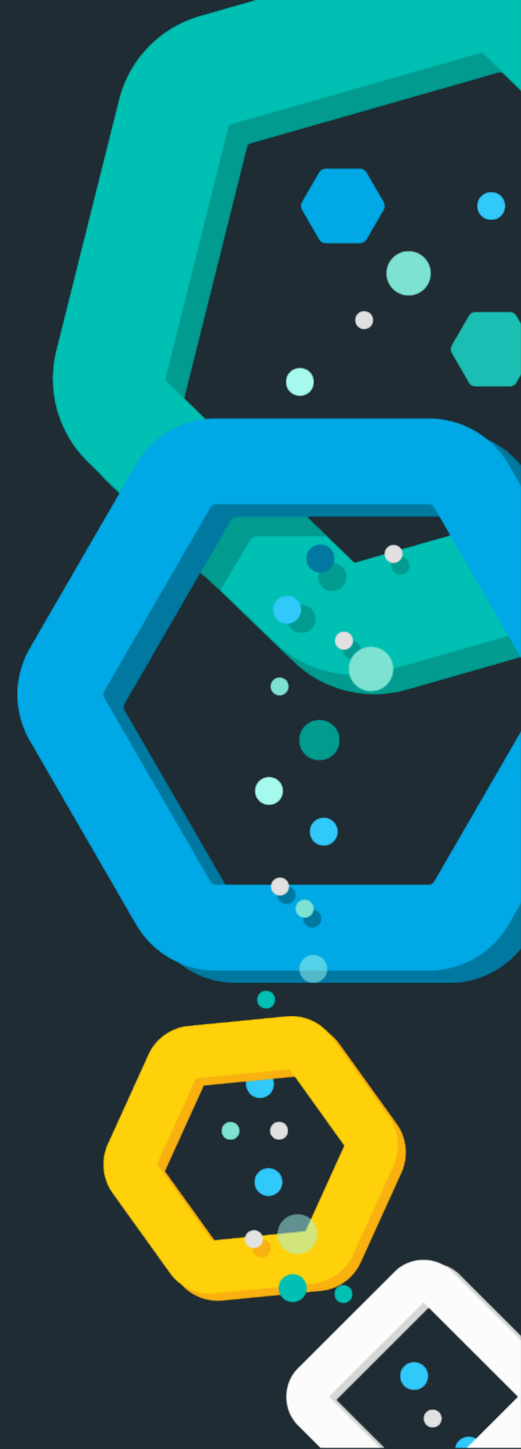
Aggregations

- bucket: terms, histogram, geo, range, sampler , significant text, nested
- metric: value_count, avg, min, max, sum, stats, median deviation, geo, percentile, cardinality,
- pipeline: min, max, sum, avg, derivative, stats, percentiles, cumulative sum, moving average, moving function, serial differencing

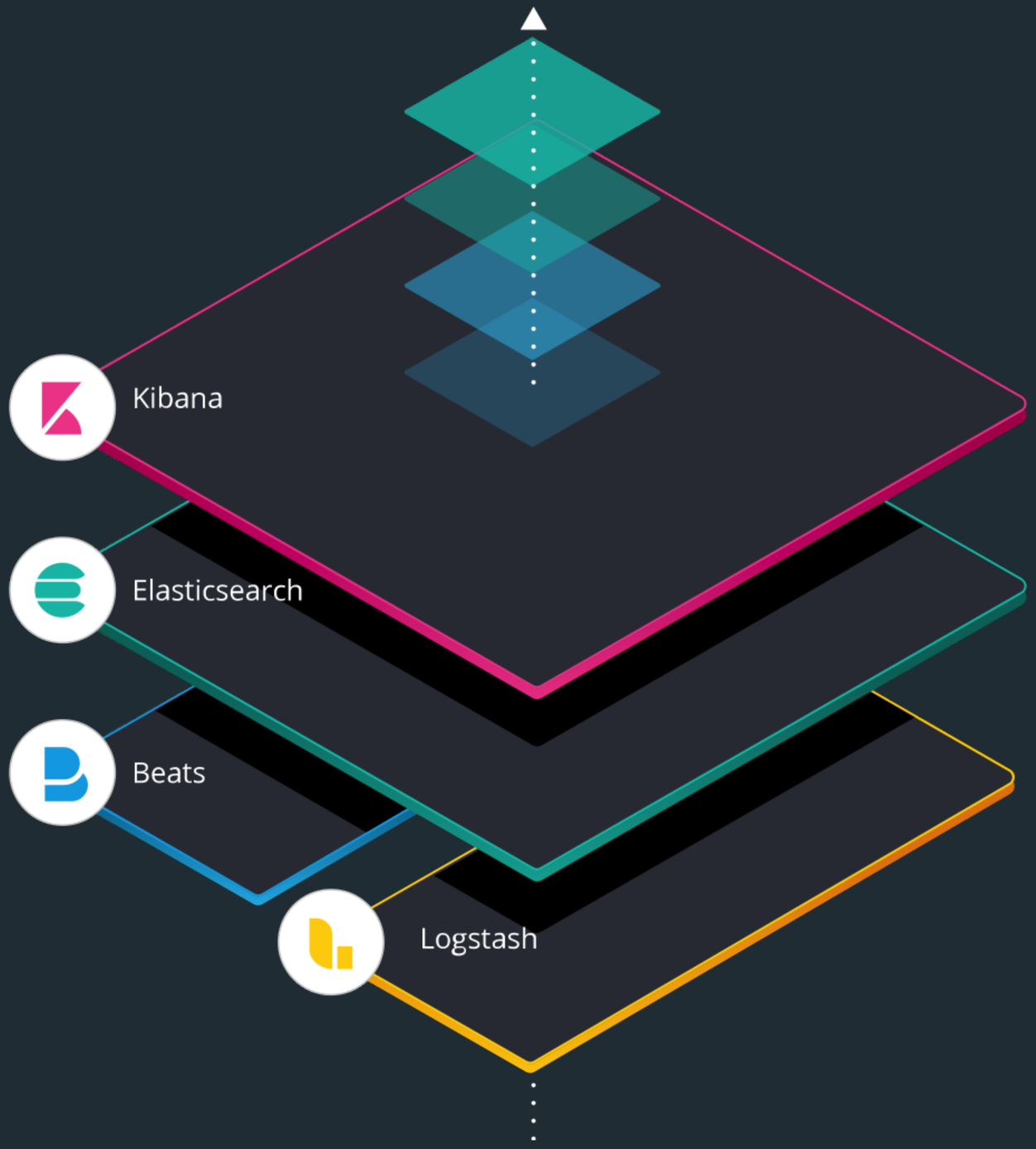
elastic

Distributed systems & search

Fanning out a search, reducing the results



Elasticsearch

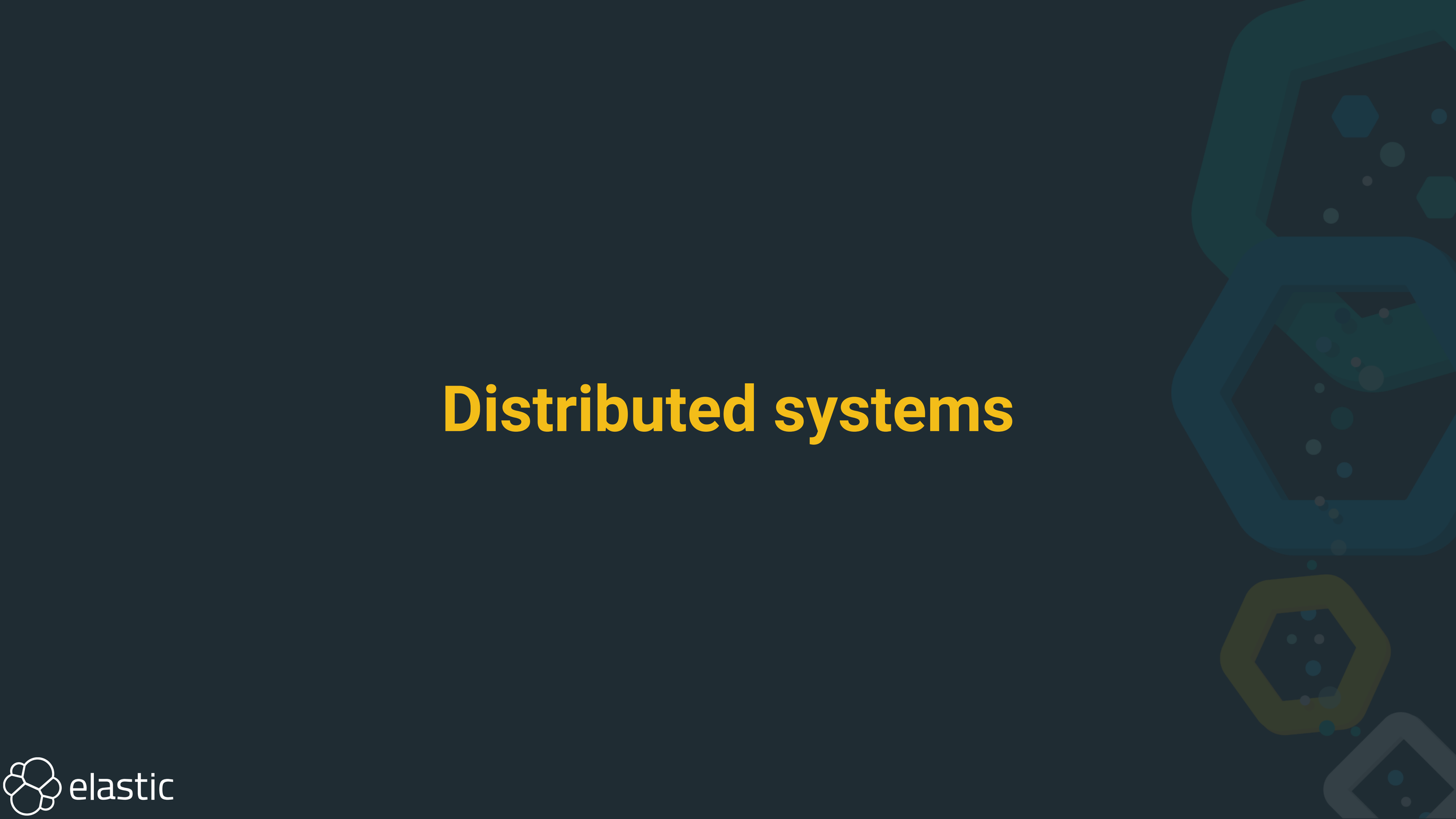


elastic

Elasticsearch in 10 seconds

- Search Engine (FTS, Analytics, Geo), near real-time
- Distributed, scalable, highly available, resilient
- Interface: HTTP & JSON
- Centrepiece of the Elastic Stack
- Uneducated conservative guess: Tens of thousands of clusters worldwide, hundreds of thousands of instances

Distributed systems



elastic

Distributed systems

- How do nodes communicate with each other?
- Who is taking and executing decisions?
- Failure detection?
- Replication strategy?
- Consistency?
- Enter consensus algorithms...

elastic

A fundamental problem in distributed computing and multi-agent systems is to achieve overall system reliability in the presence of a number of faulty processes. This often requires processes to agree on some data value that is needed during computation

https://en.wikipedia.org/wiki/Consensus_(computer_science)

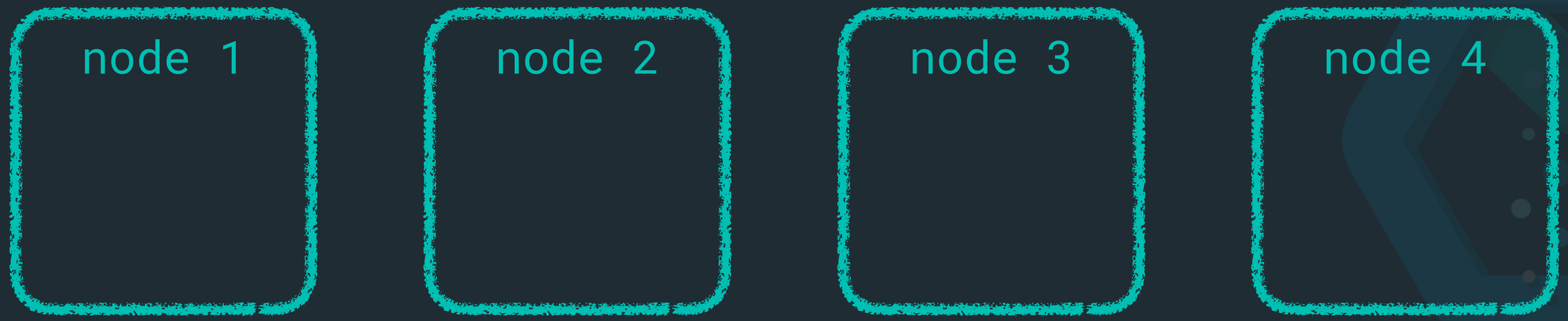
Consensus algorithms

- Leader based: Paxos, Raft
- Non leader based: BTC, gossip

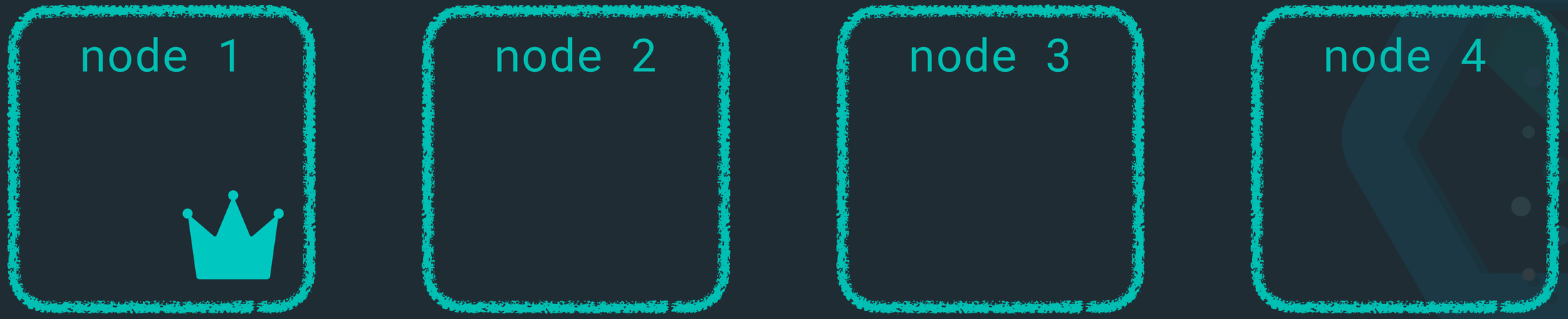
Consensus in Elasticsearch

- Custom consensus algorithm, improving the existing one
- Formally verified
- Optimized for Elasticsearch use-case (rolling restarts, growing/shrinking clusters, log-of-operations vs. cluster state)

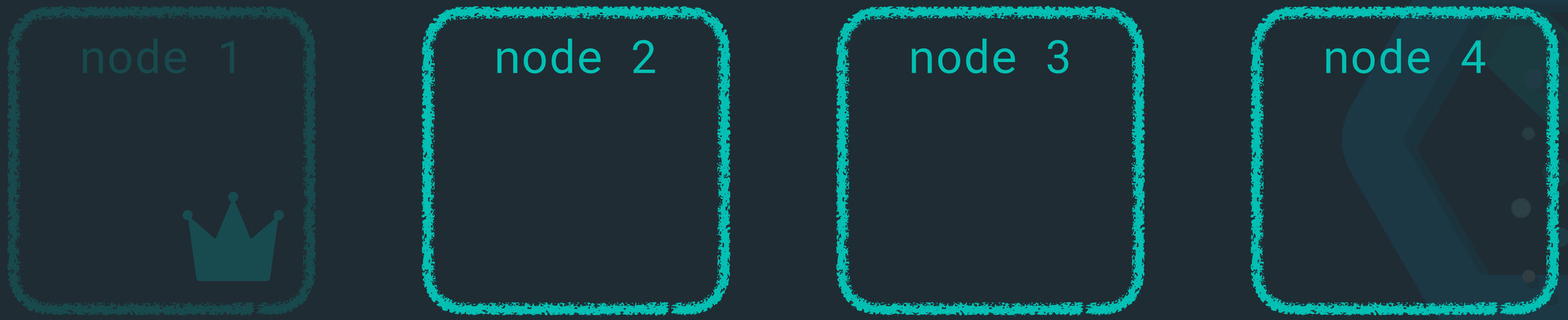
Consensus in Elasticsearch



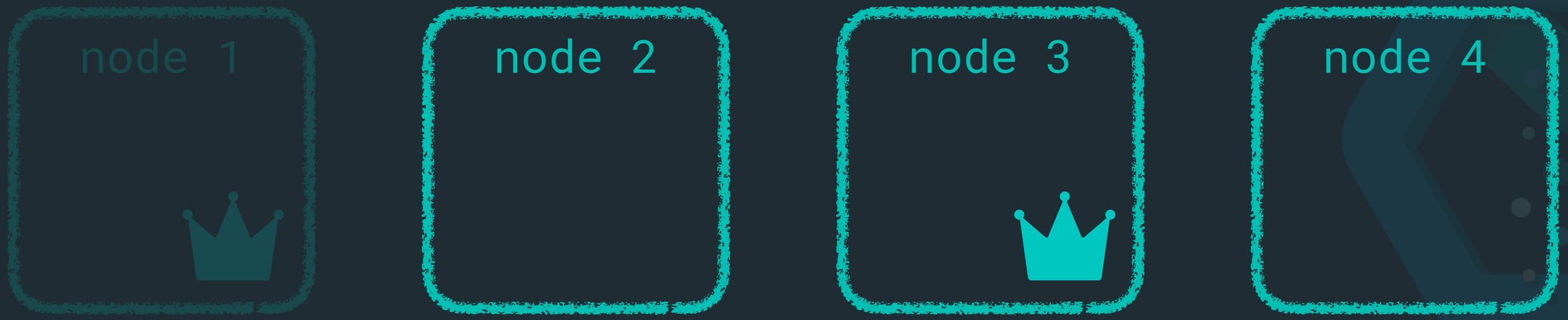
Consensus in Elasticsearch



Consensus in Elasticsearch



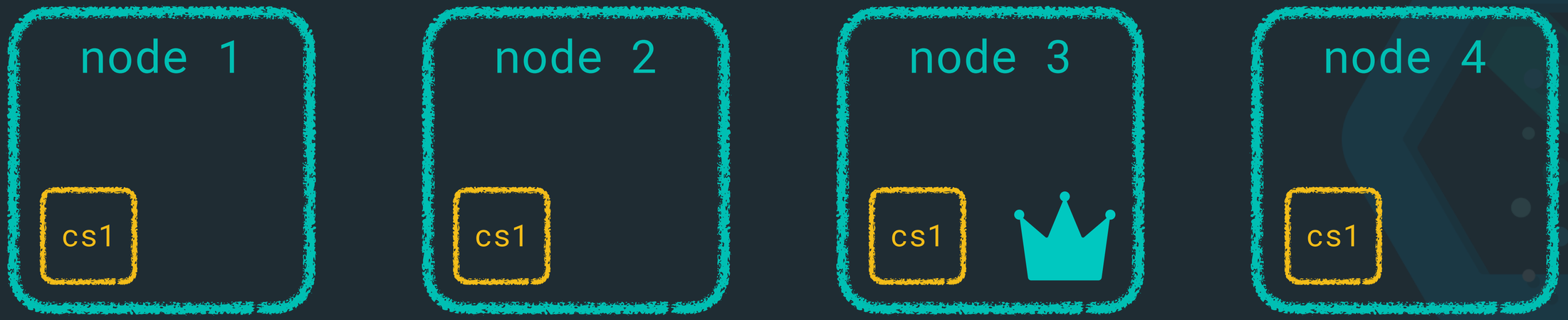
Consensus in Elasticsearch



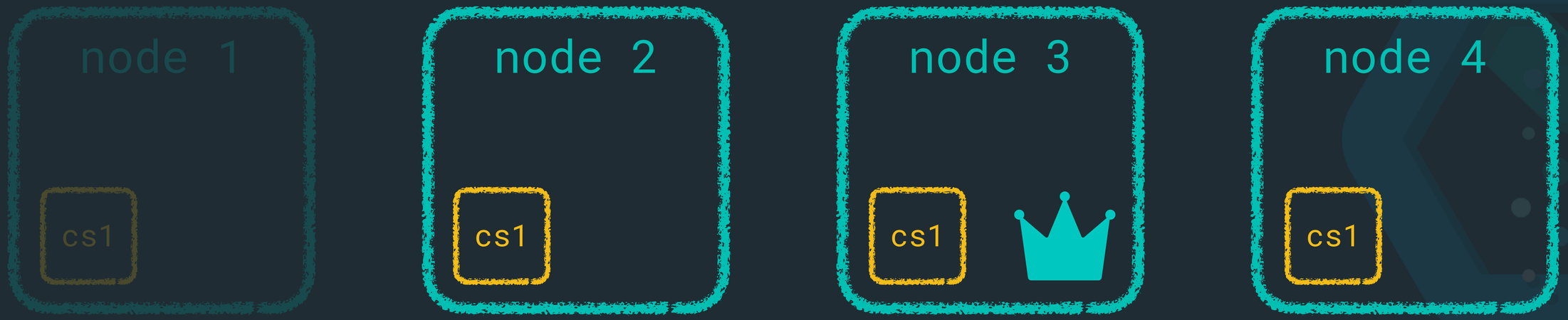
Master node tasks

- Deciding where data should be stored
- Pinging other nodes
- Reacting on node leaves/joins
- Updating cluster state
- Distributing cluster state

Consensus in Elasticsearch

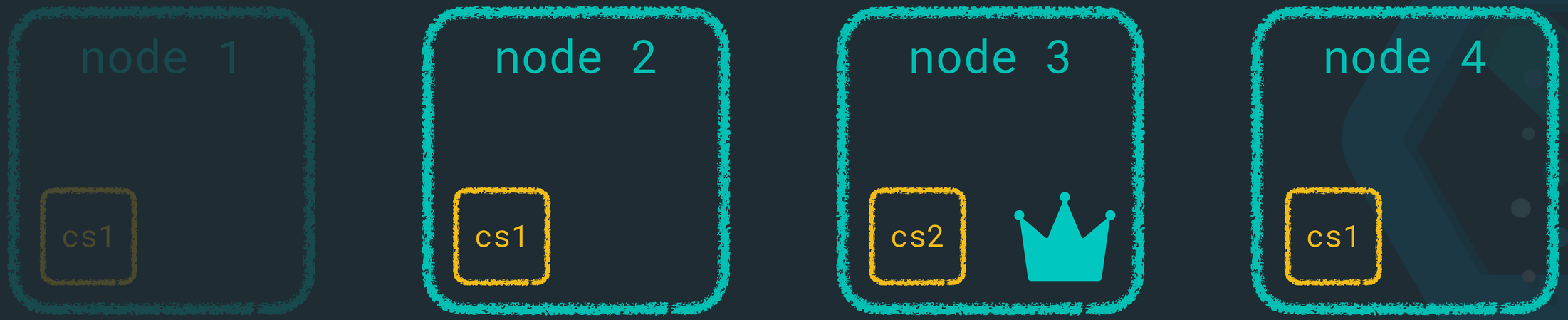


Consensus in Elasticsearch



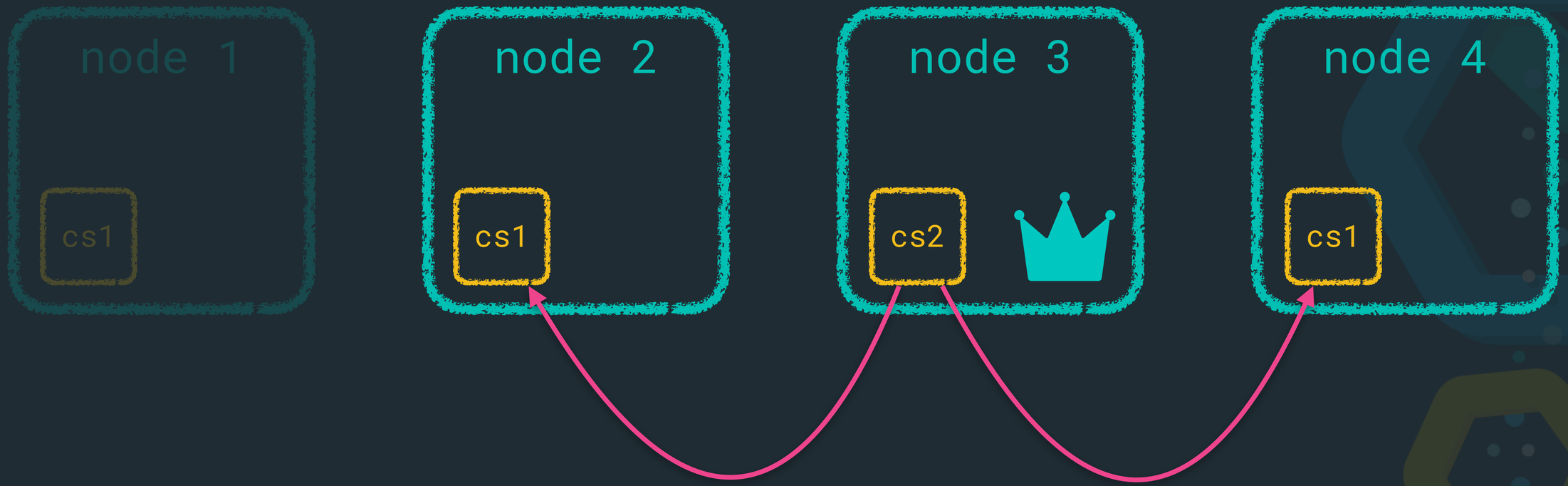
elastic

Consensus in Elasticsearch

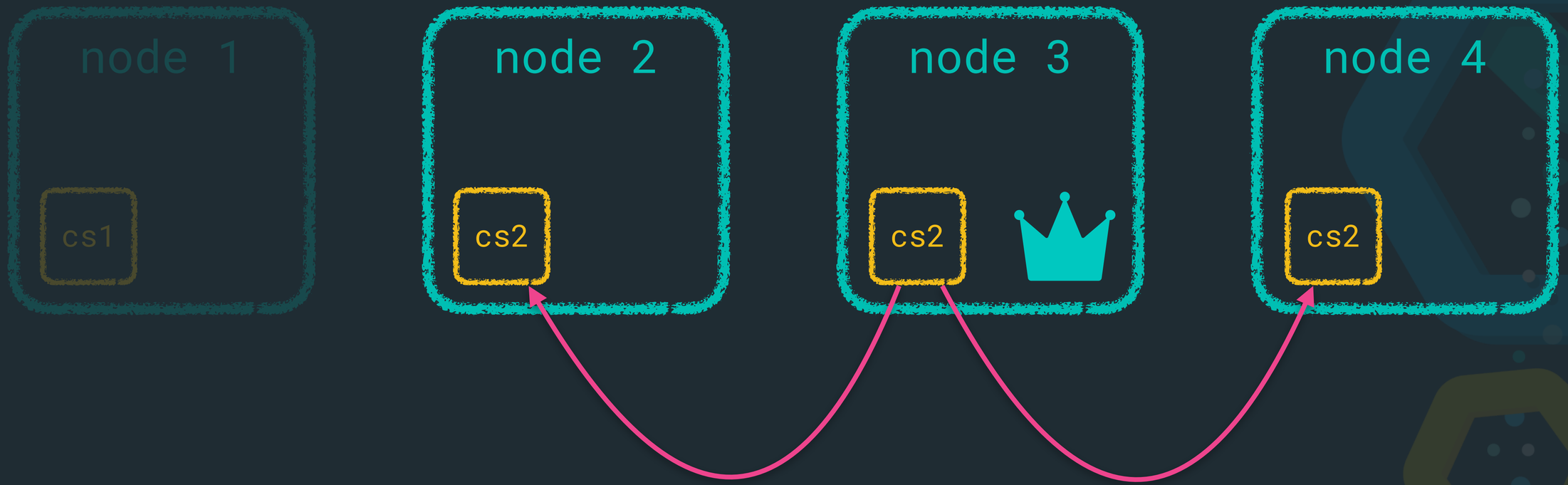


elastic

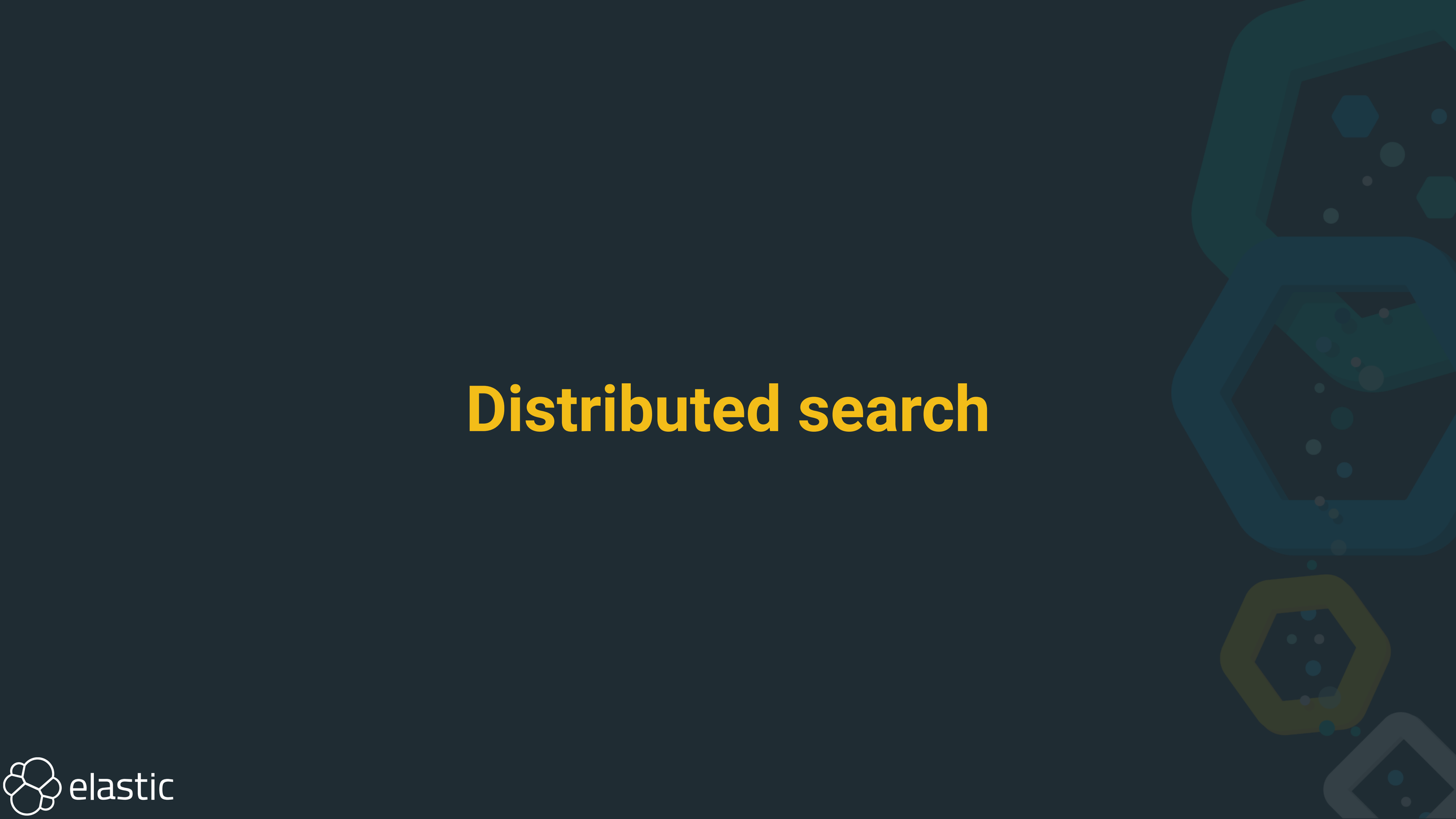
Consensus in Elasticsearch



Consensus in Elasticsearch

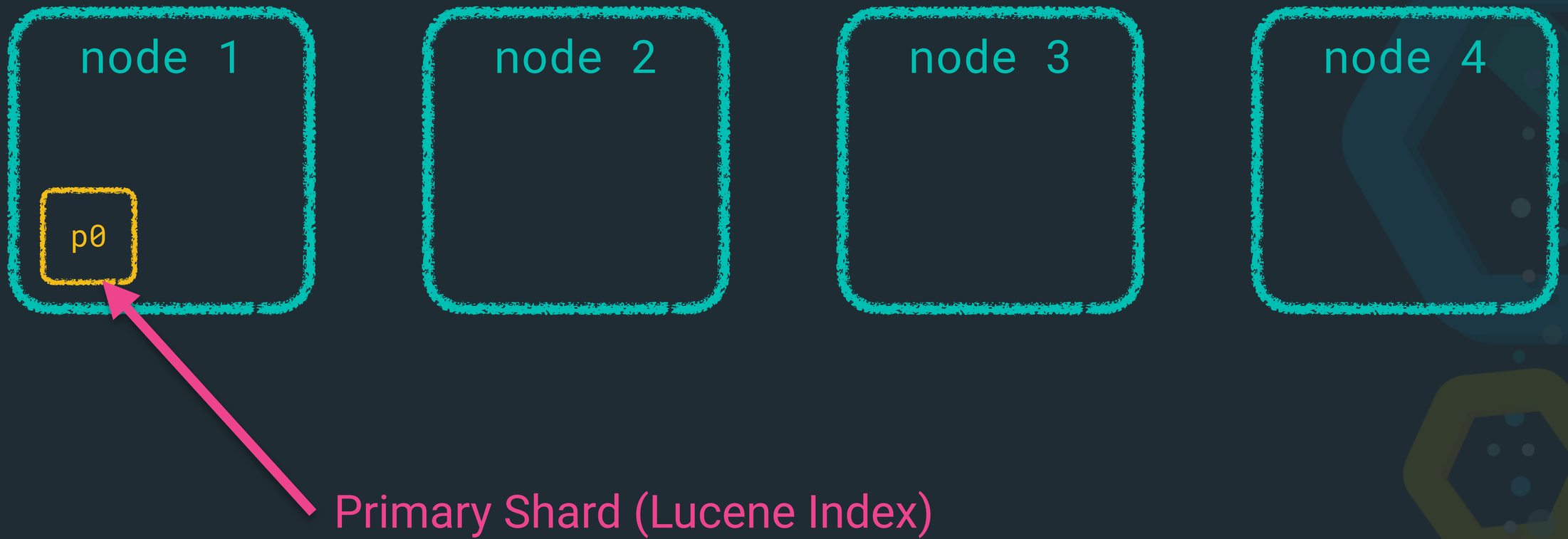


Distributed search



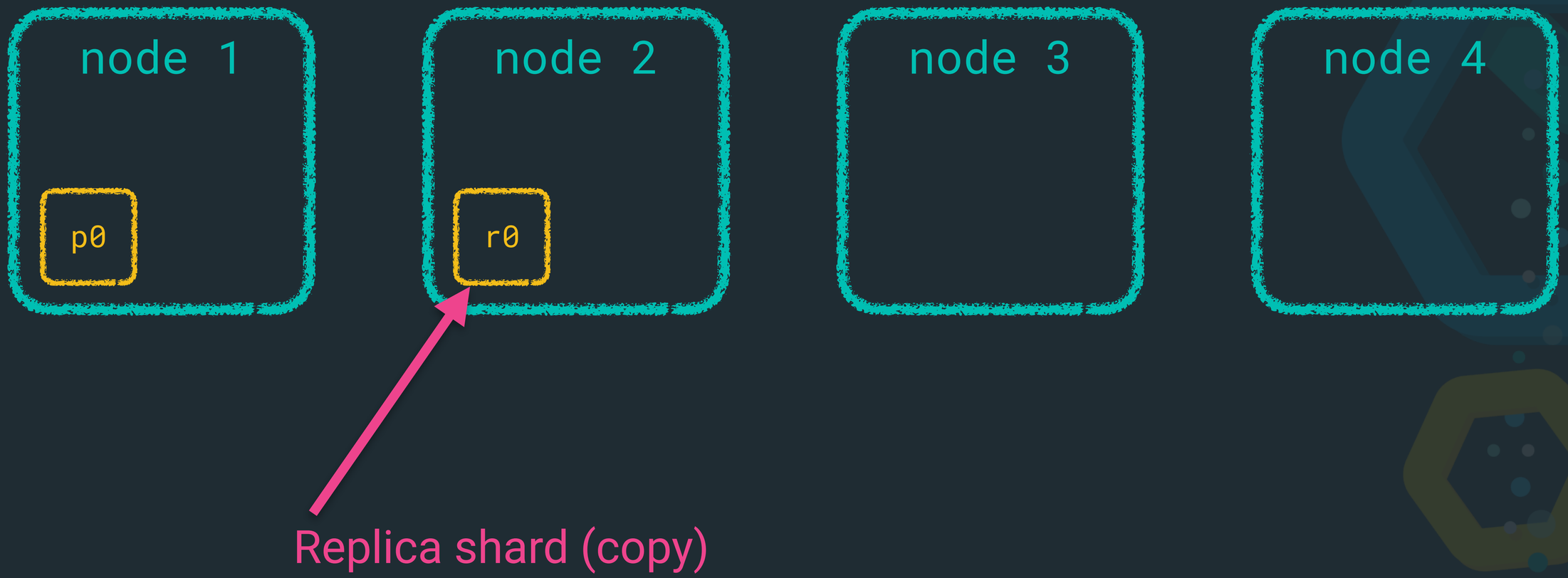
elastic

Distributed search in Elasticsearch



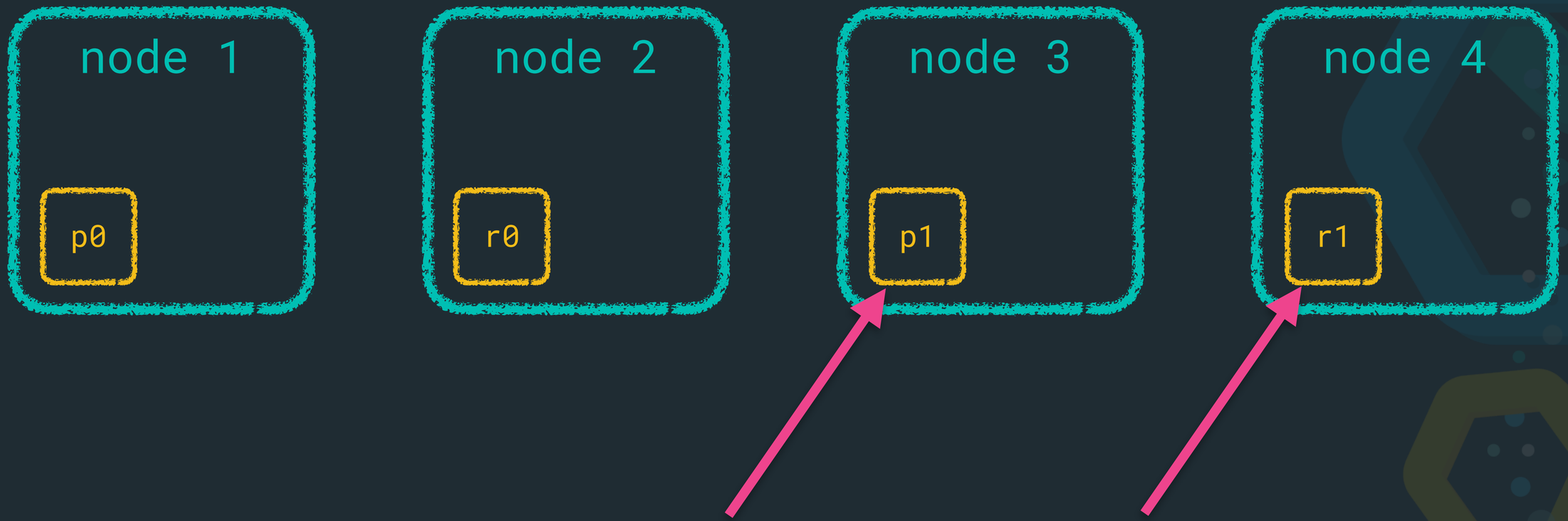
elastic

Distributed search in Elasticsearch



elastic

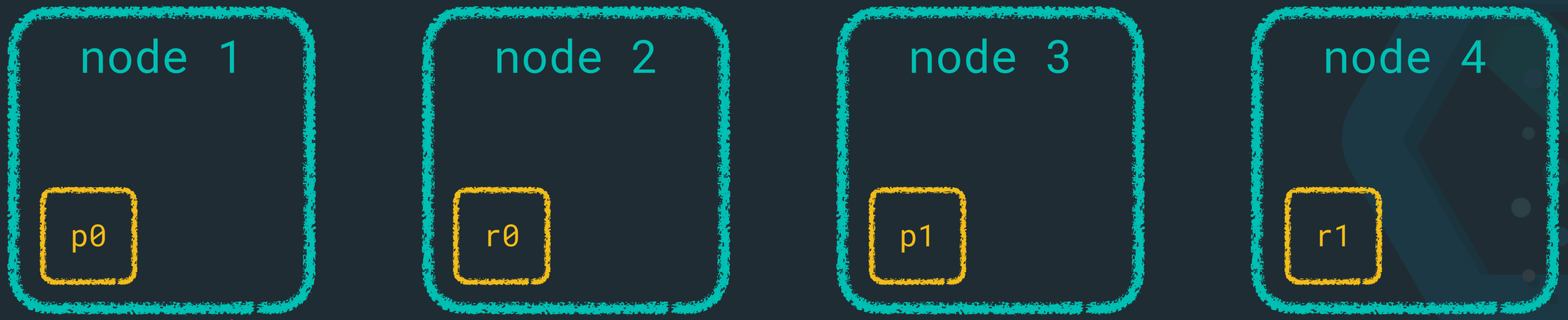
Distributed search in Elasticsearch



Distributed search in Elasticsearch

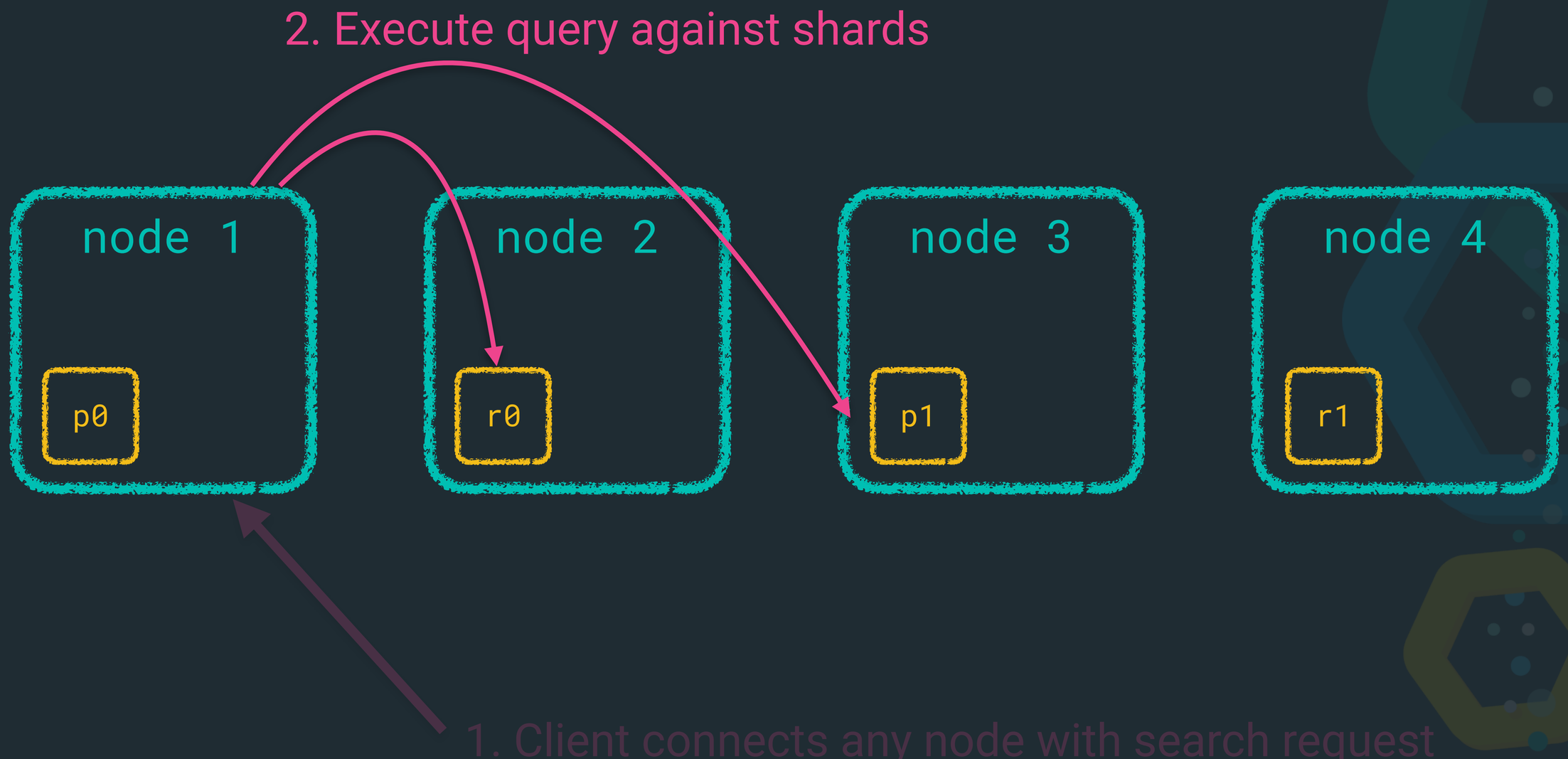
- Shard: Lucene index, unit of scale
- Primary shard: Write scalability
- Replica shard: Read scalability, availability

Distributed search in Elasticsearch



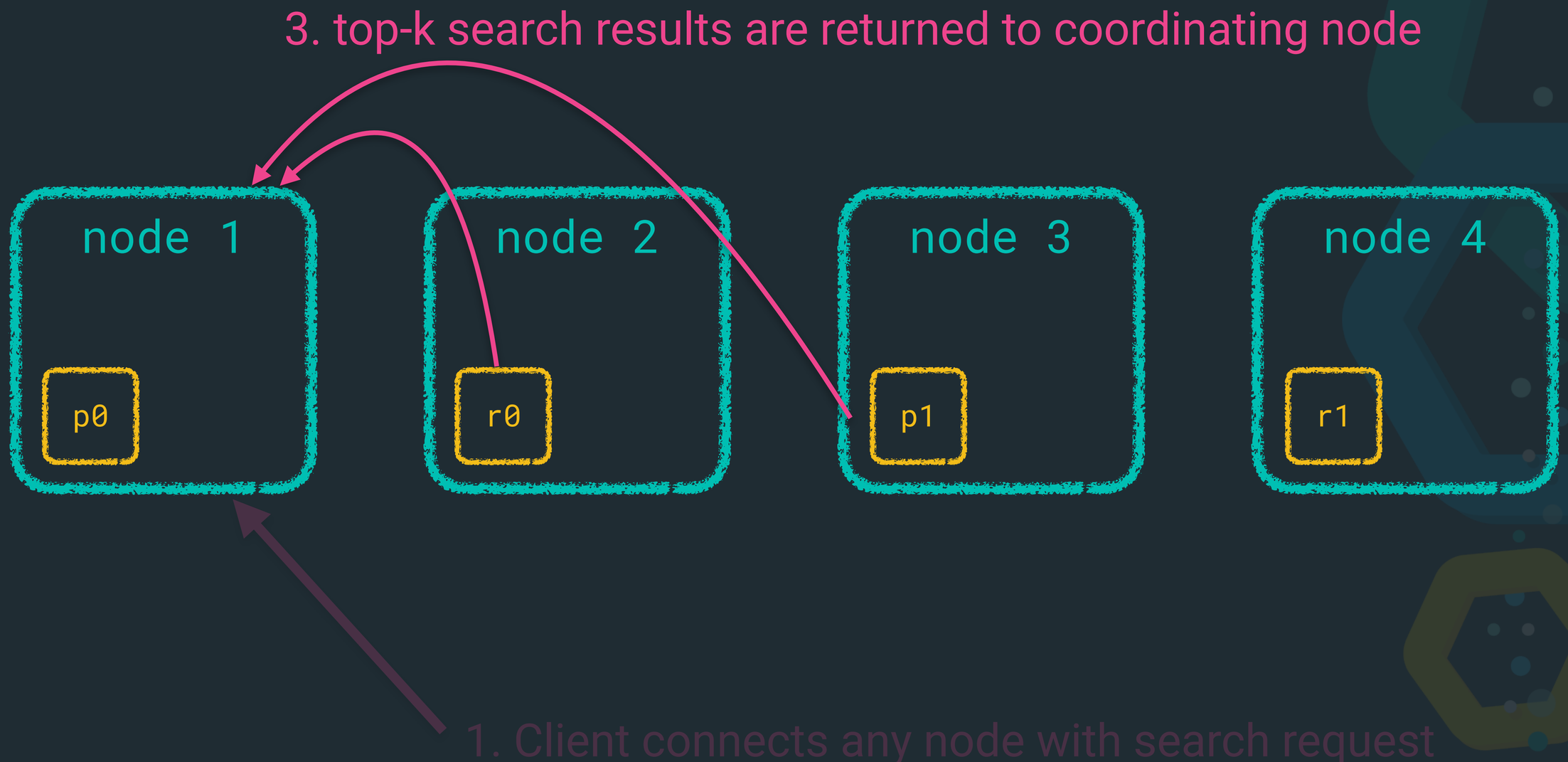
1. Client connects any node with search request

Distributed search in Elasticsearch



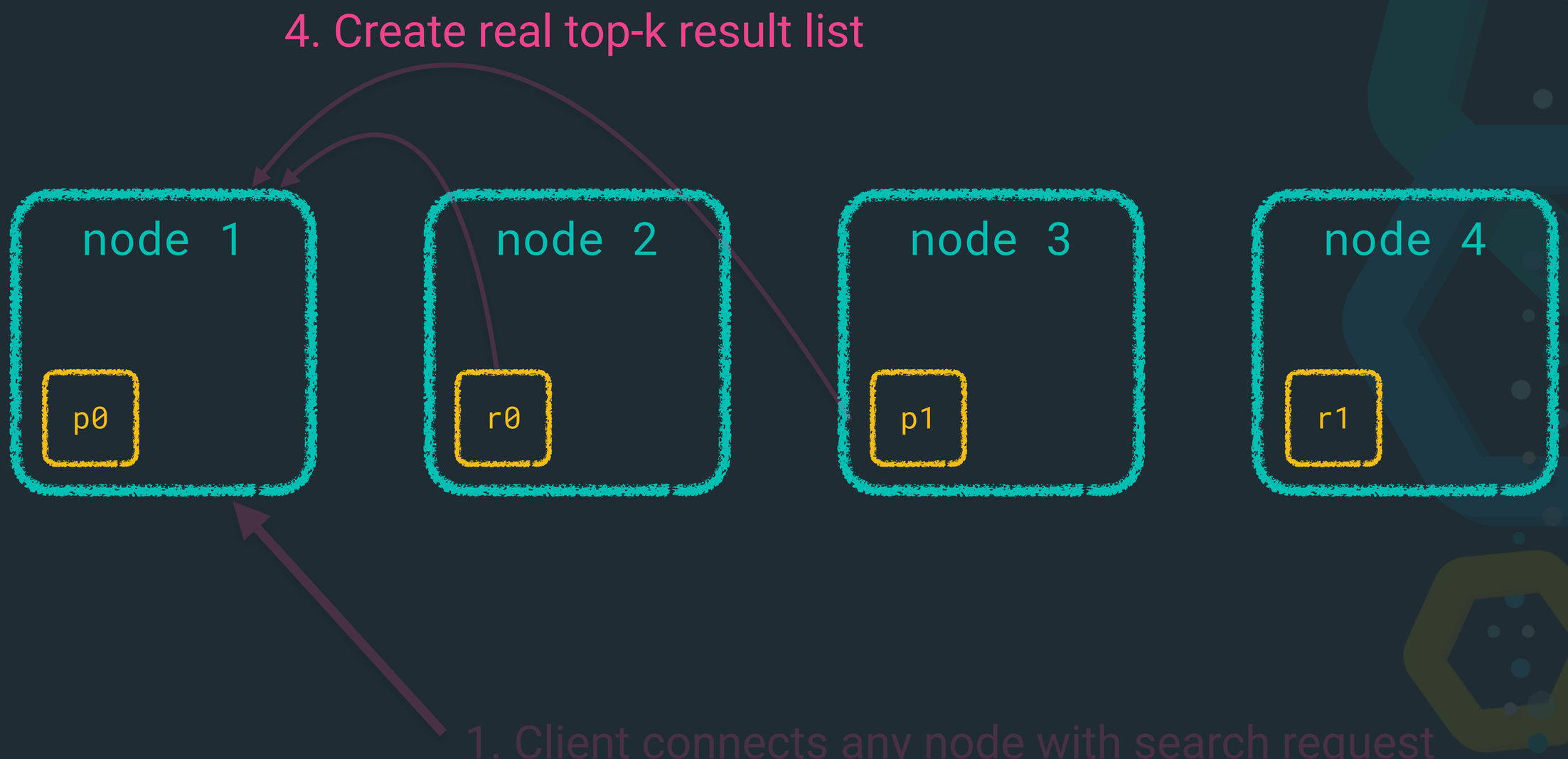
elastic

Distributed search in Elasticsearch



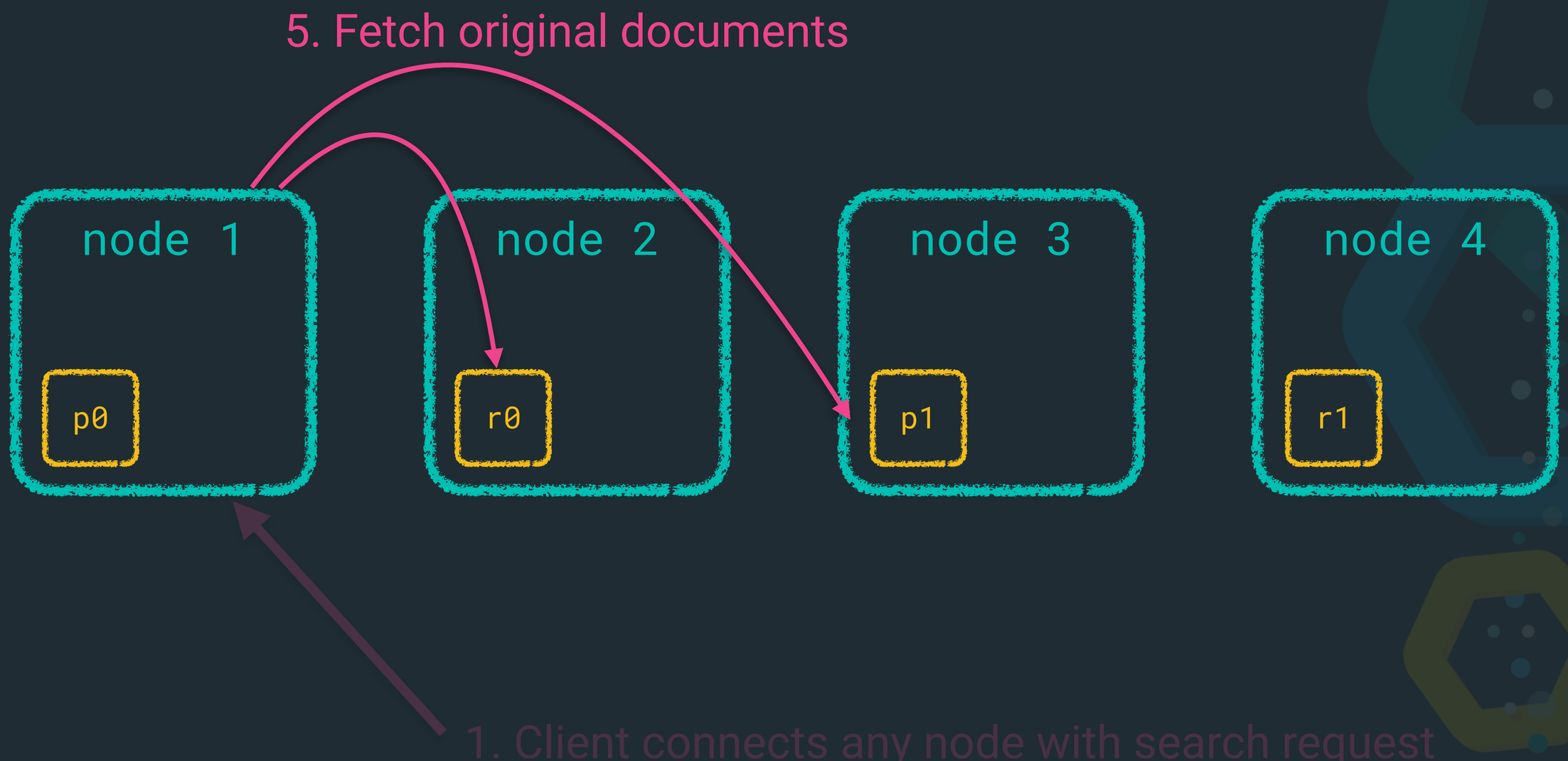
elastic

Distributed search in Elasticsearch



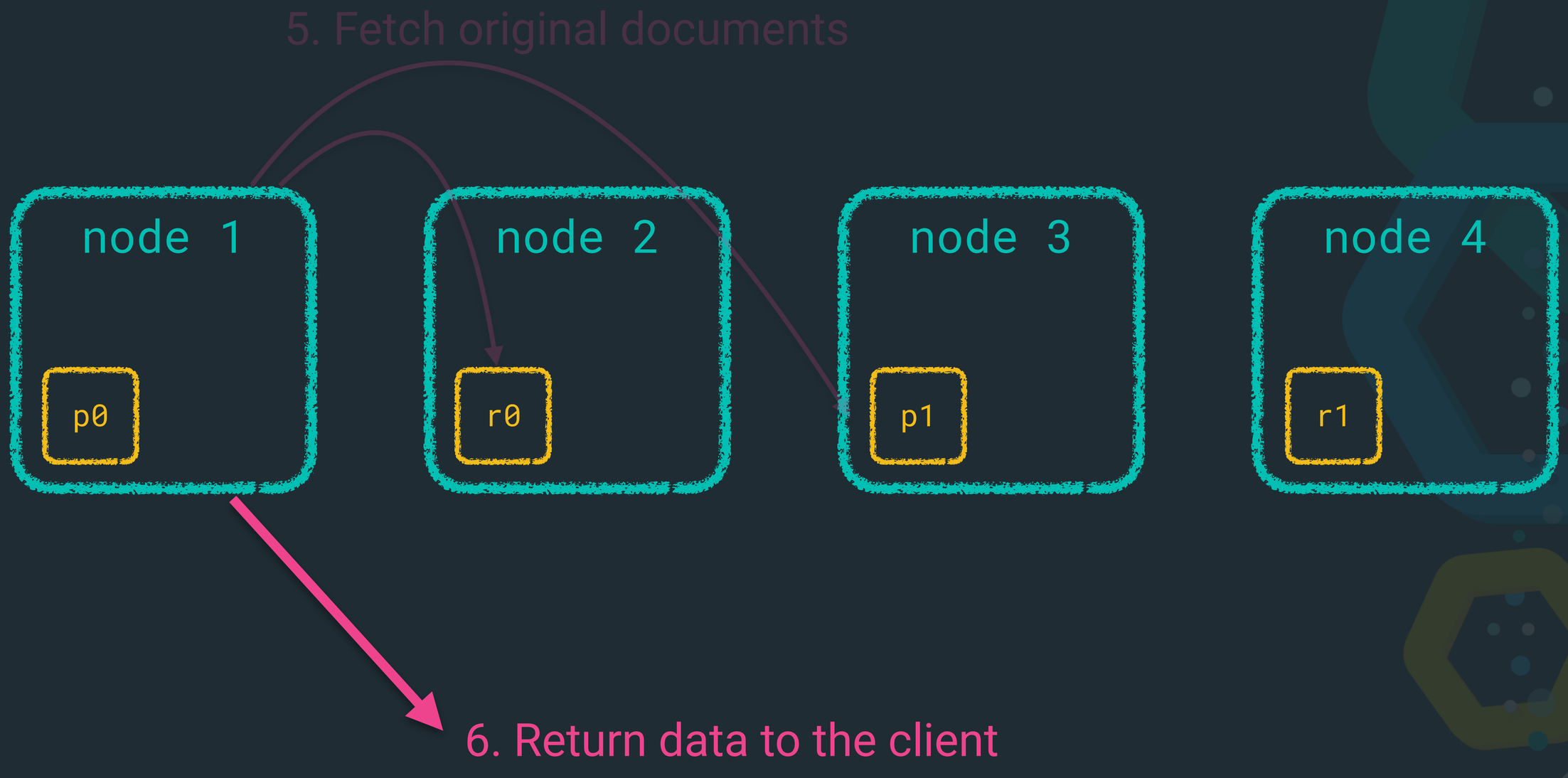
elastic

Distributed search in Elasticsearch



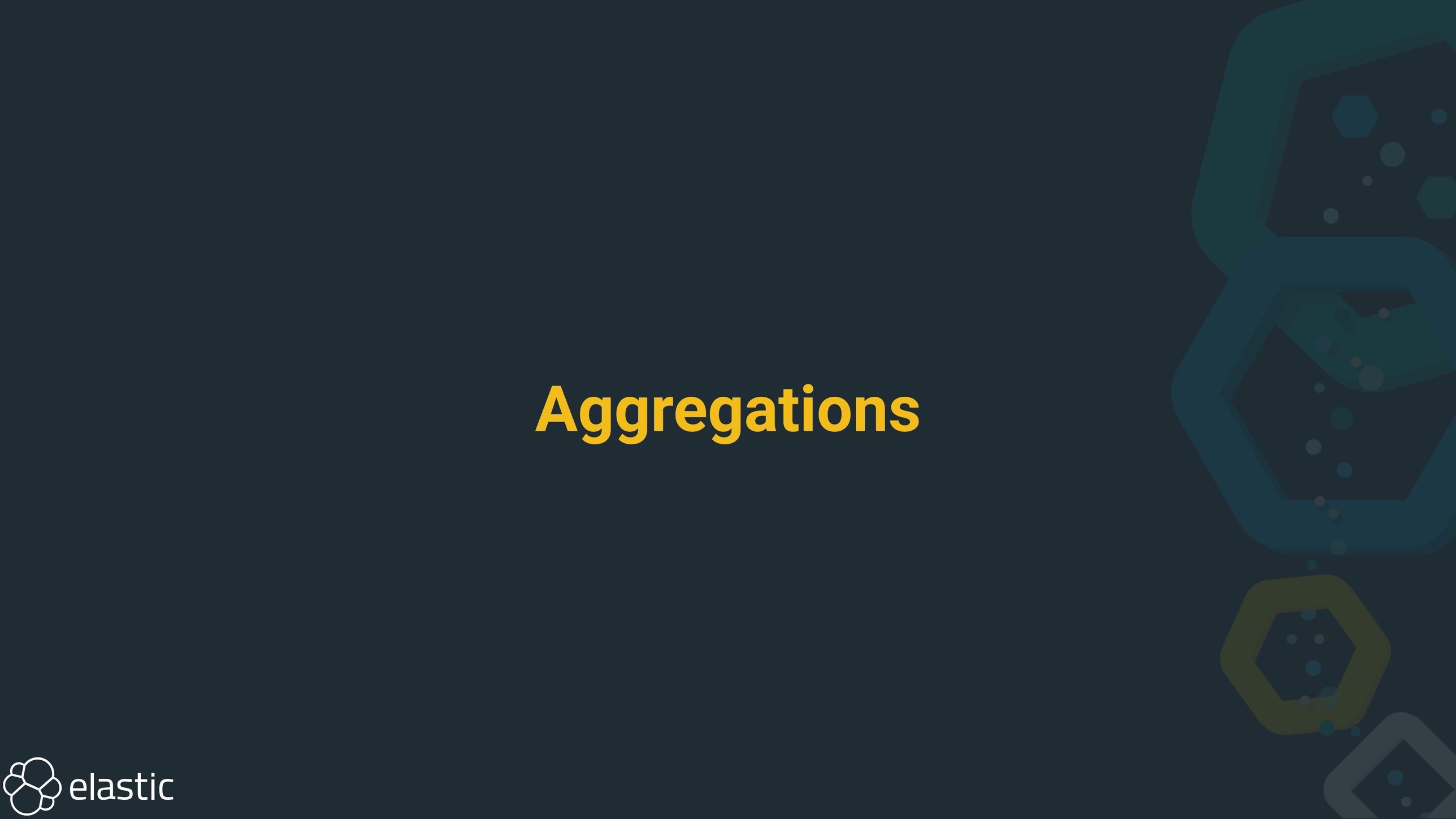
elastic

Distributed search in Elasticsearch



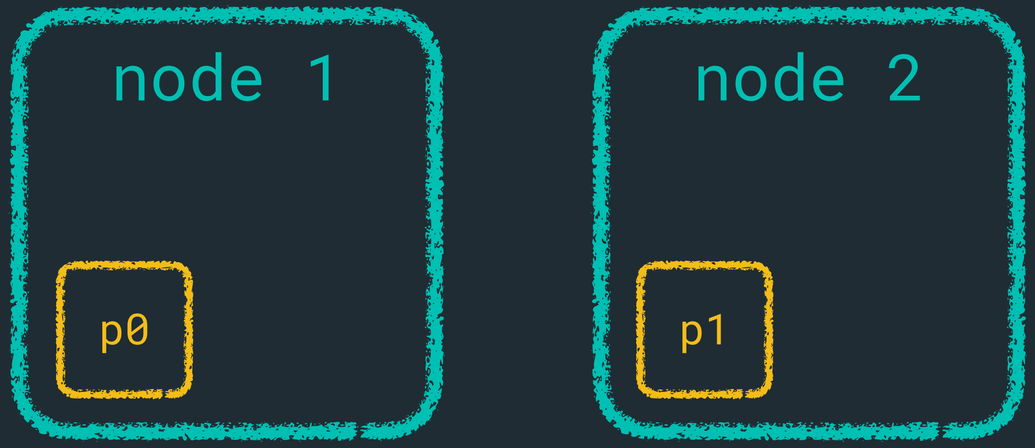
elastic

Aggregations



elastic

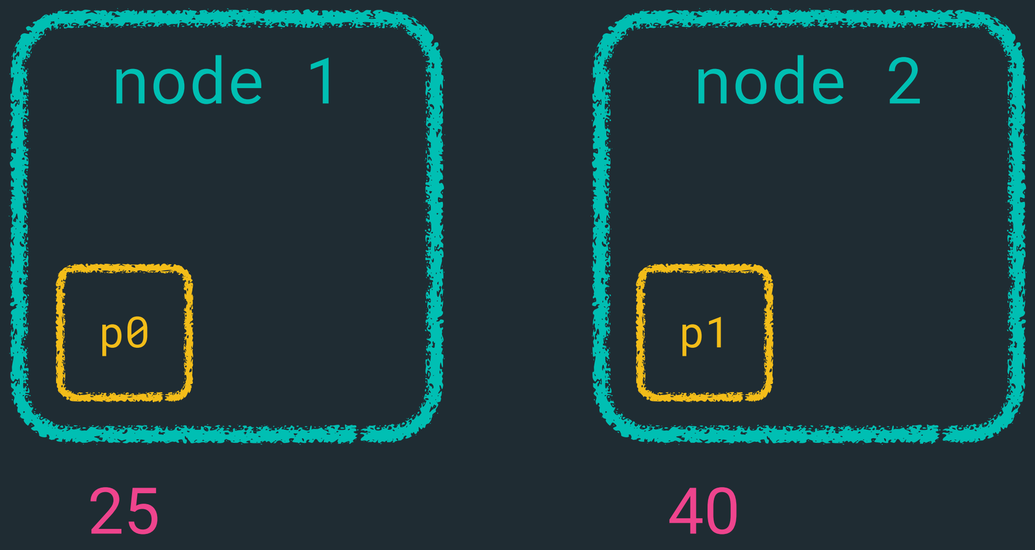
Aggregations - cardinality




```
POST /sales/_search?size=0
{
  "aggs" : {
    "type_count" : {
      "cardinality" : {
        "field" : "type"
      }
    }
  }
}
```

elastic

Aggregations - cardinality



How many distinct elements are in my index?

What is the total? 40? 65?

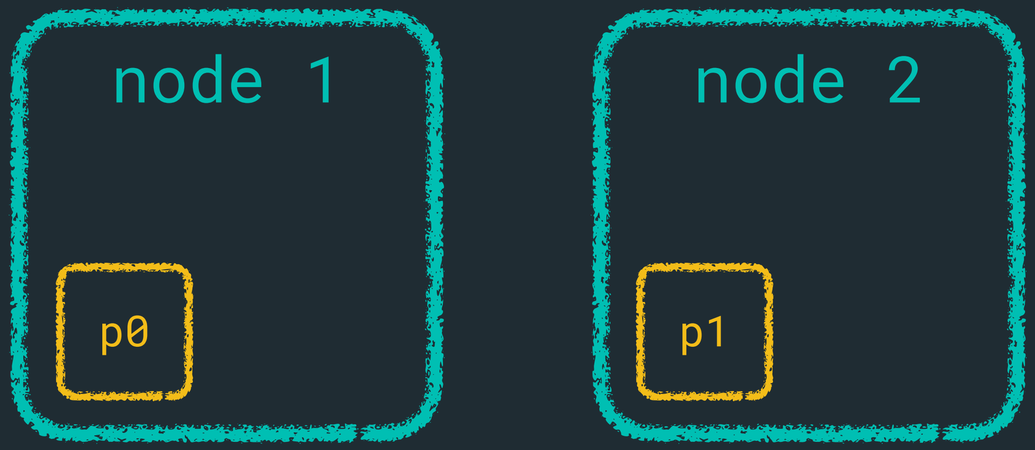
Naive solution: merge data to single dataset and count. Doesn't scale!

Solution: Use HyperLogLog++

HyperLogLog++

- Hash based counting
- Trades in memory for accuracy
- Fixed memory usage, based on configurable precision
- Result: Small mergeable data structure, can easily be sent over the network

Aggregations - percentile




```
GET latency/_search
{
  "size": 0,
  "aggs" : {
    "load_time_outlier" : {
      "percentiles" : {
        "field" : "load_time"
      }
    }
  }
}
```

elastic

T-Digest

- Extreme percentiles are more accurate than the Median
- Percentiles are divided into buckets
- When buckets grow over a boundary, approximation kicks in, saving memory in the process
- The exact level of inaccuracy is difficult to generalize
- Alternative: HDR histograms

Probabilistic data structures

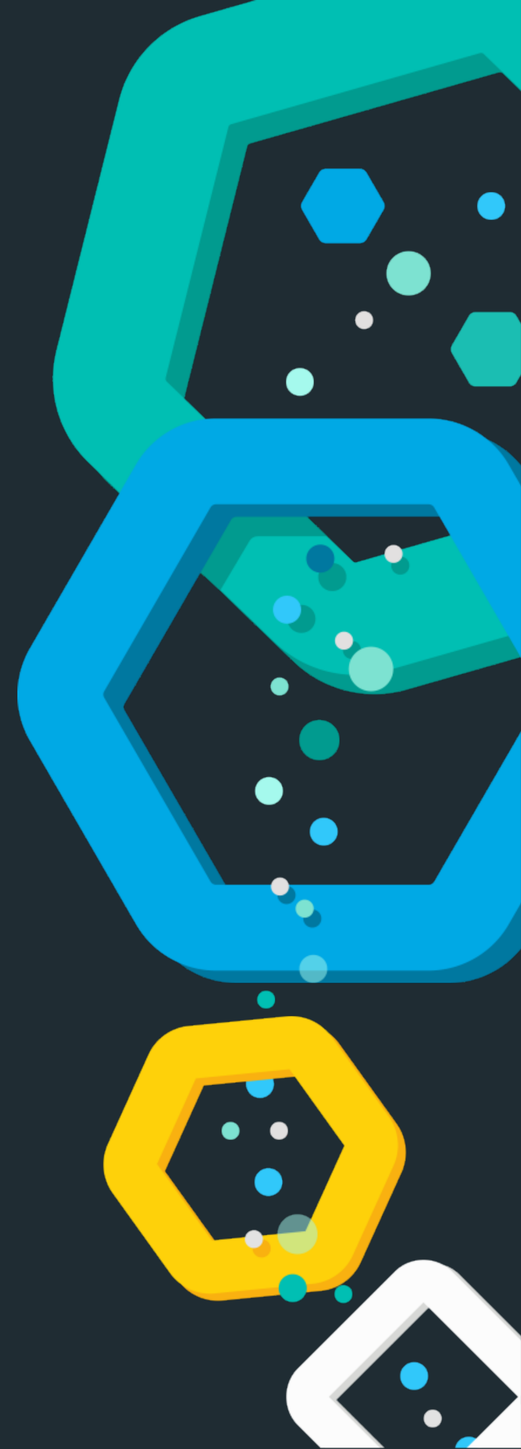
- bloom/cuckoo/quotient filters (membership check)
- HyperLogLog++ (cardinality)
- T-Digest, DDSketch, HDR histogram (percentile)
- Count-Min sketch (frequency, top-k)
- Hashing (similarity)

elastic

Demo

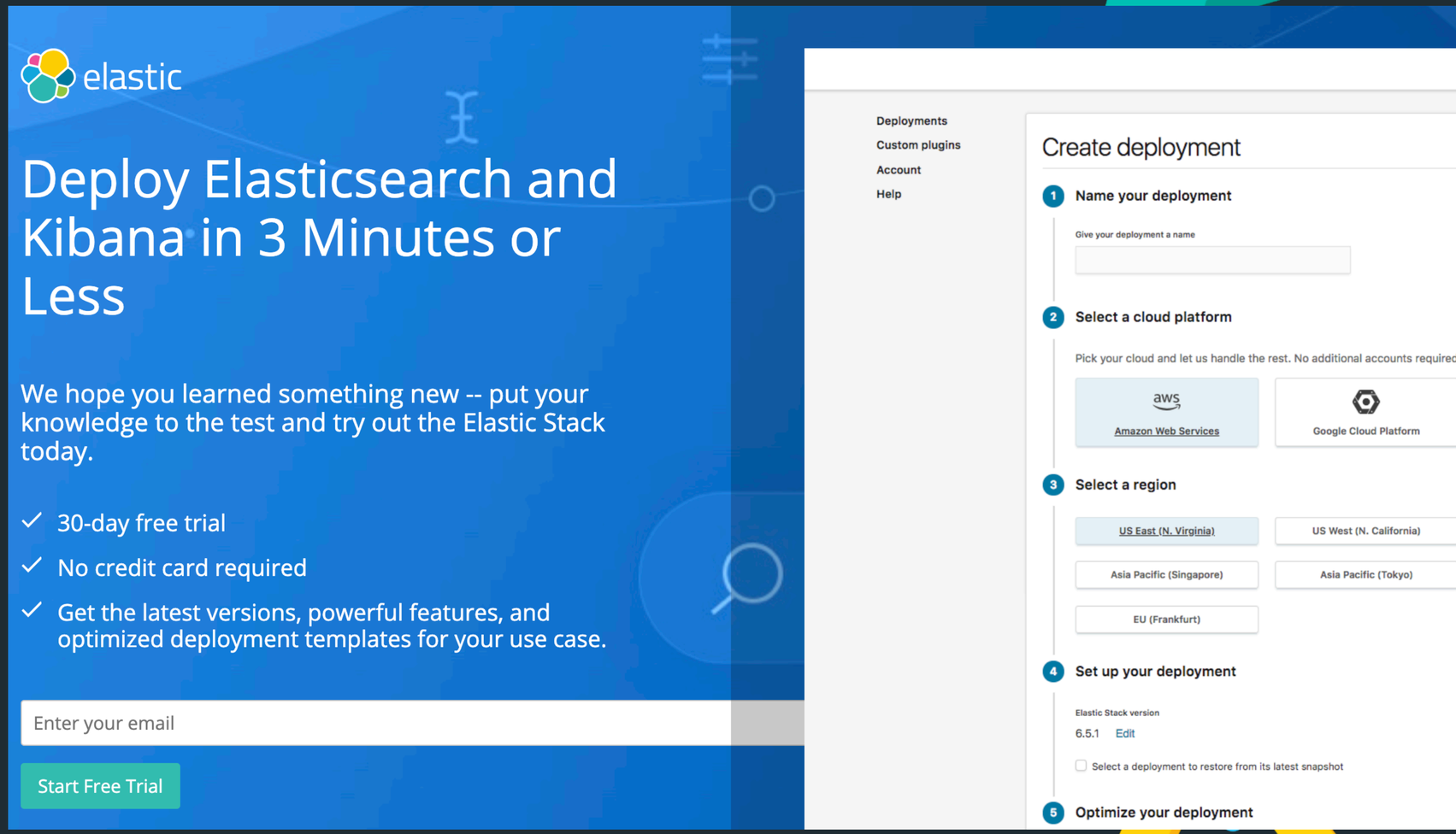
Try it out yourself!

https://ela.st/jade-hochschule-samples



elastic

Elastic Cloud
Free 30 day trial

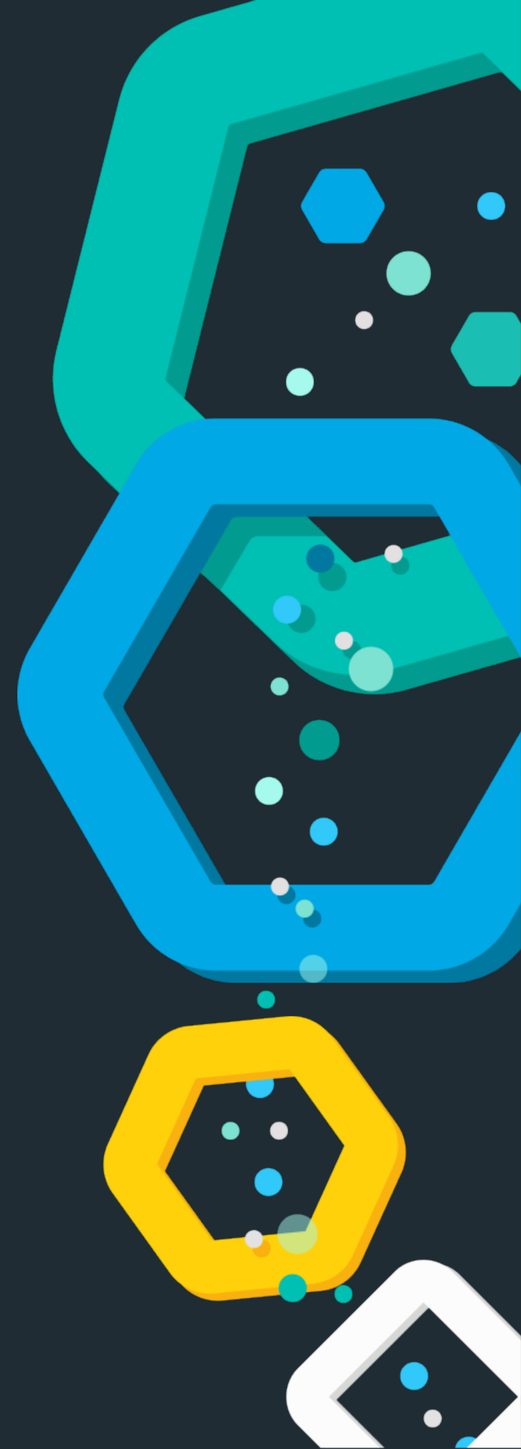


https://ela.st/hack-your-future-2020

elastic

Upcoming trends & summary

... or why you should take a closer look at search



Search is not just google...

- "Just google it" does not cut it
- Enterprise search: Intranet/G-Drive/Dropbox
- Ecommerce search
- SIEM
- Observability: Logging, APM & Metrics

Search is not 'done'

- Constant improvement
- Data structures & algorithms (BKD tree for geo shapes)
- Academic research moves to industry thanks to Apache Lucene

Search is still tough

- Language specific analysis
- Smart query parsing (`nike red hoodie xl`)
- Geo based search
- Anomaly detection
- Incoporating feedback loops

Upcoming trends

- Learning-to-Rank
- Deep Learning
- Feedback loop

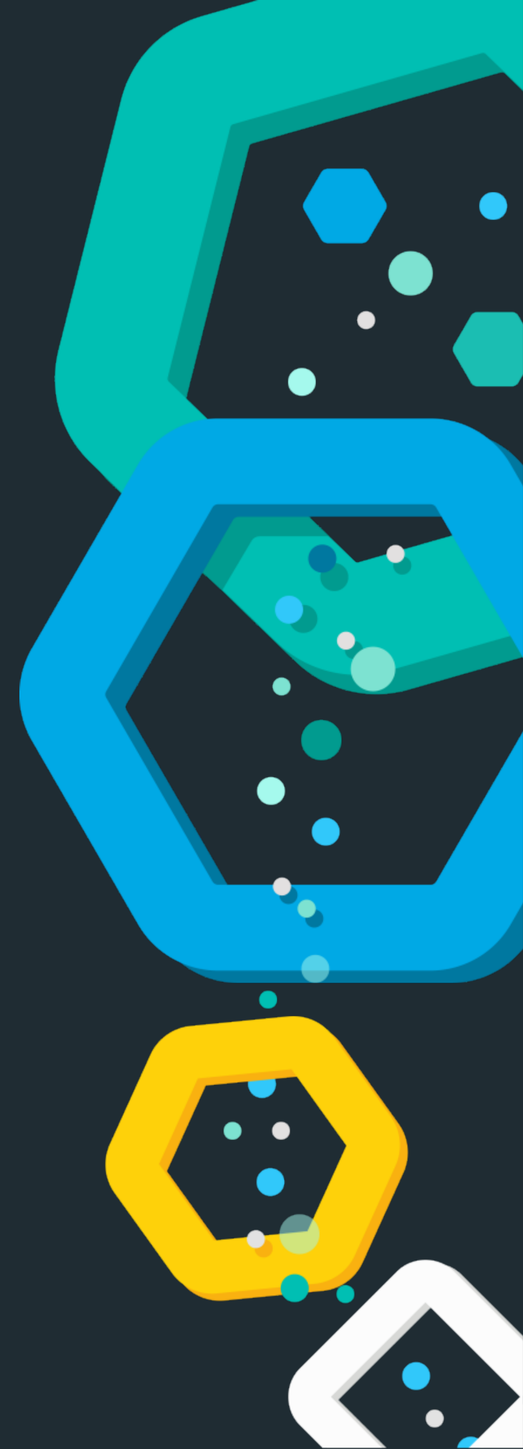
Summary

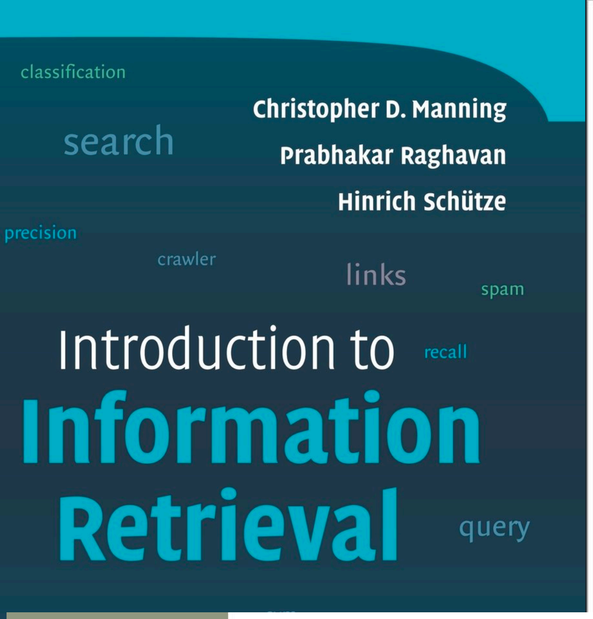
- Everything is a search problem!
- Search is hard... and interesting
- Distributed systems are hard... and interesting
- Domain knowledge required
- Data keeps exploding, good job chances!

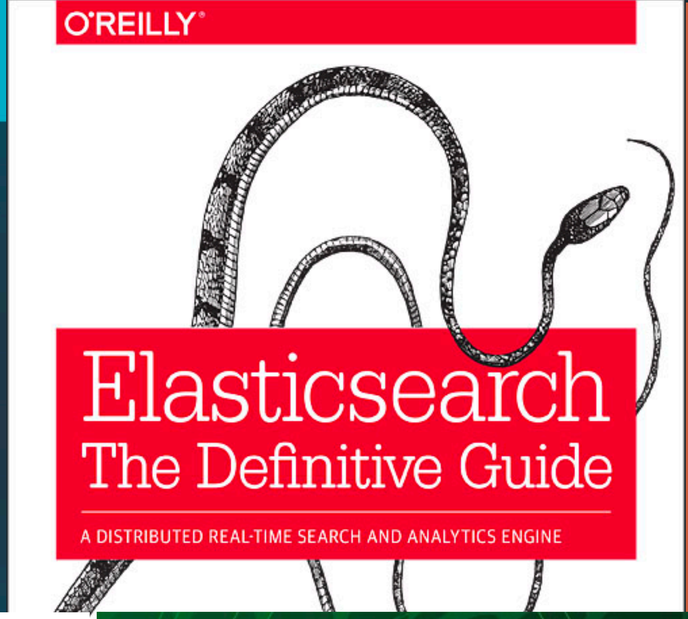
elastic

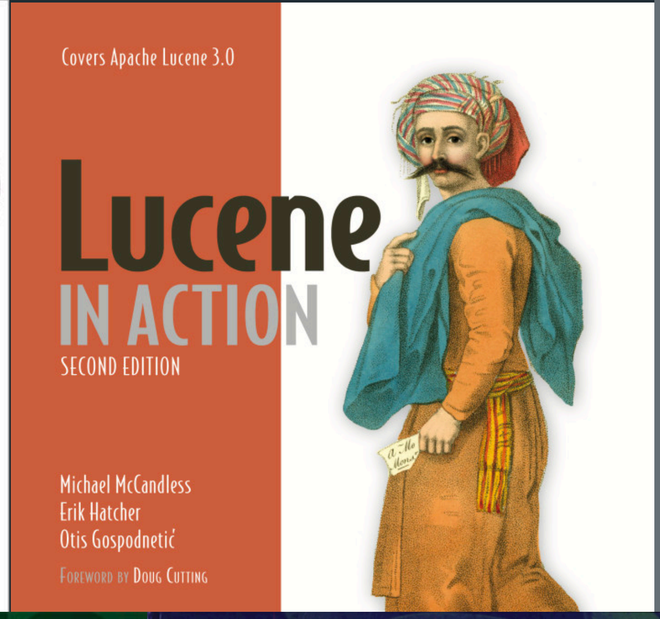
Literature

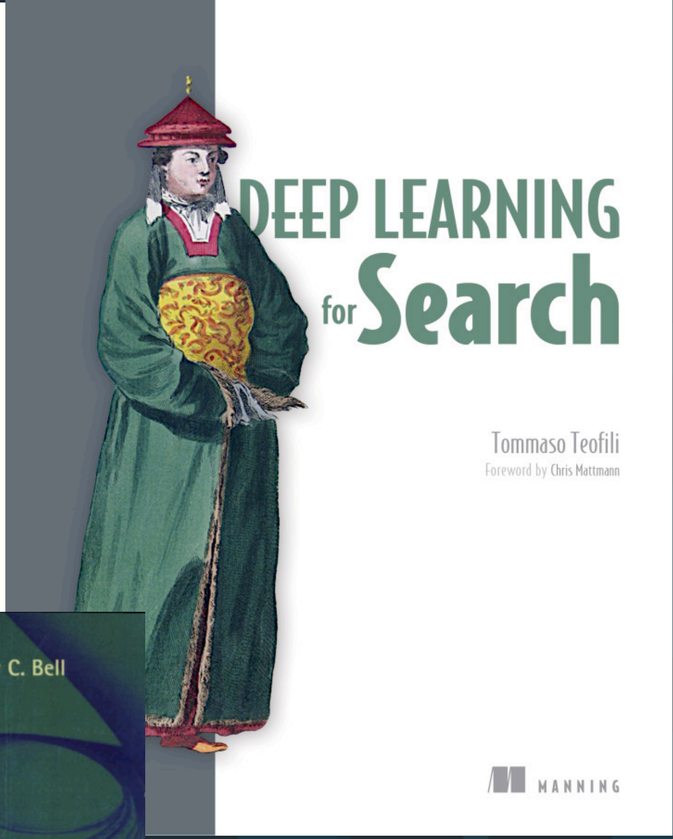
Books, books, books

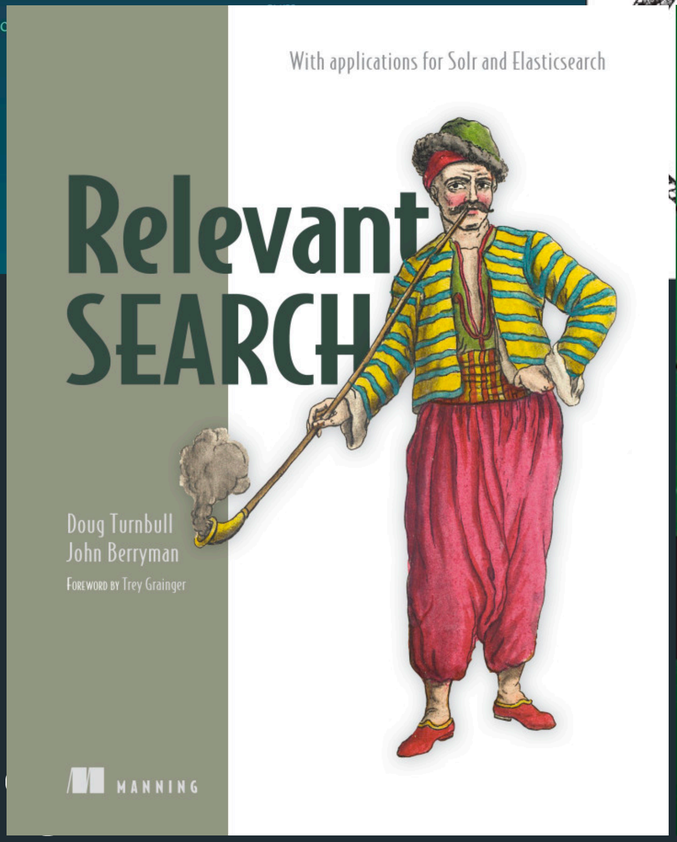


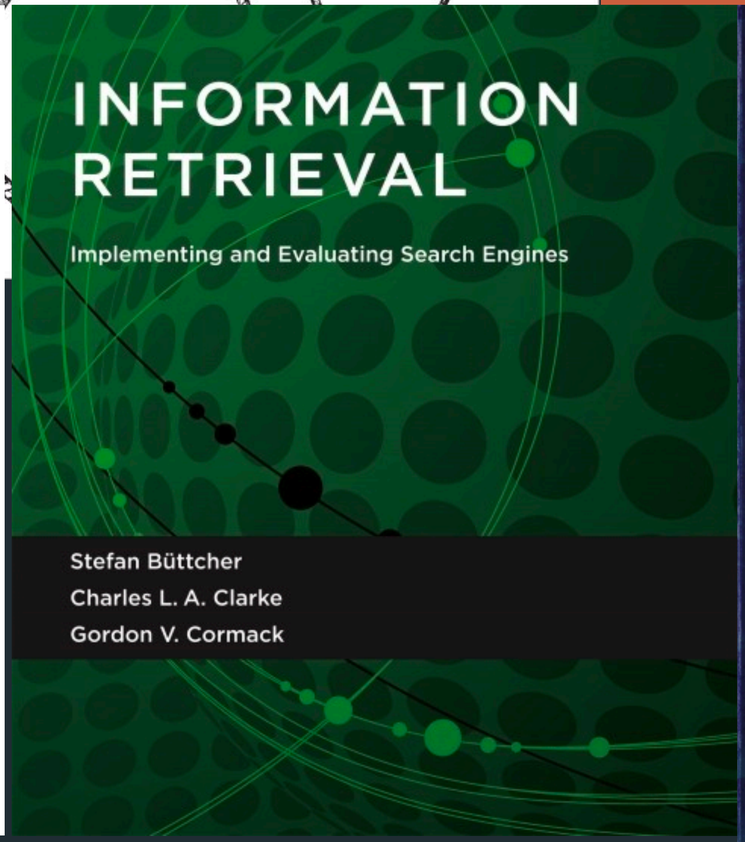

classification
search
Christopher D. Manning
Prabhakar Raghavan
Hinrich Schütze
precision
crawler
links
spam
Introduction to
recall
Information
Retrieval
query

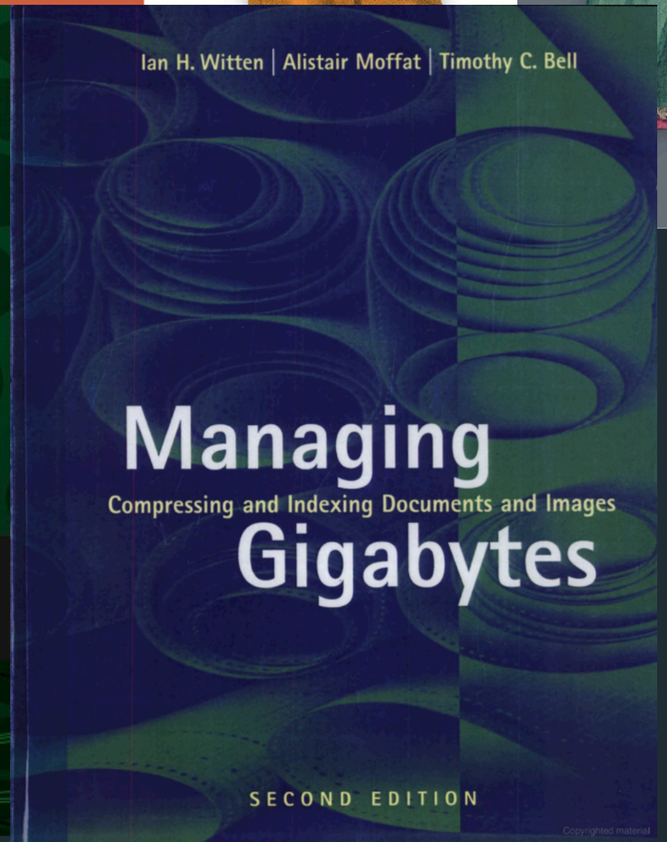

O'REILLY
Elasticsearch
The Definitive Guide
A DISTRIBUTED REAL-TIME SEARCH AND ANALYTICS ENGINE


Covers Apache Lucene 3.0
Lucene
IN ACTION
SECOND EDITION
Michael McCandless
Erik Hatcher
Otis Gospodnetić
Foreword by Doug Cutting


DEEP LEARNING
for Search
Tommaso Teofili
Foreword by Chris Mattmann
MANNING


With applications for Solr and Elasticsearch
Relevant
SEARCH
Doug Turnbull
John Berryman
Foreword by Trey Grainger
MANNING

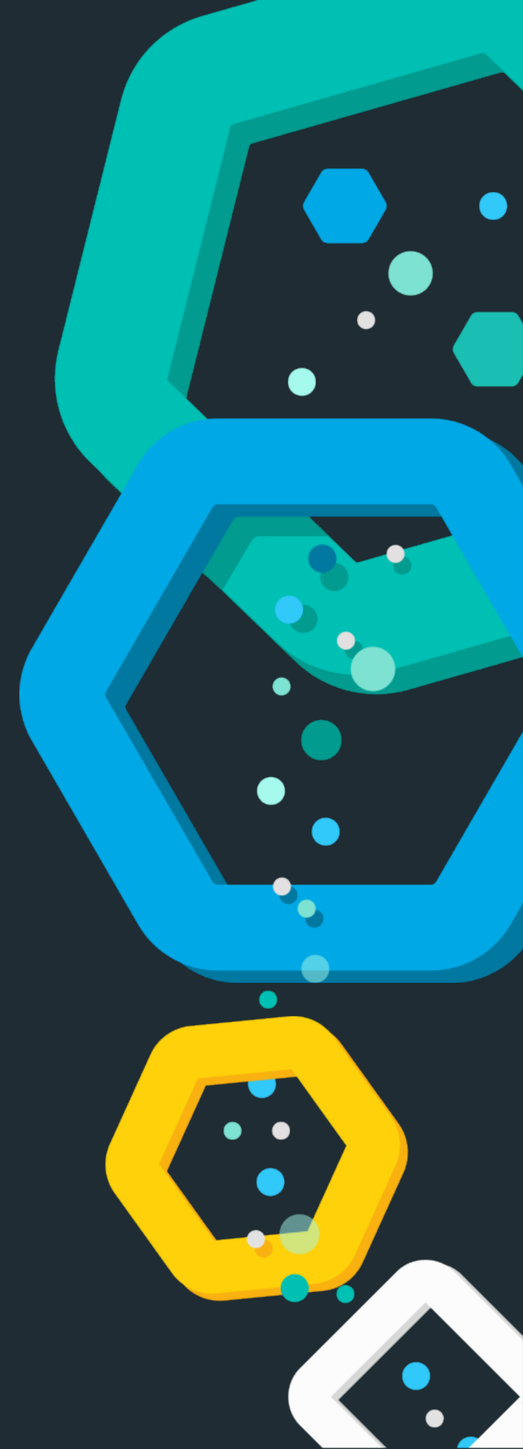

INFORMATION
RETRIEVAL
Implementing and Evaluating Search Engines
Stefan Büttcher
Charles L. A. Clarke
Gordon V. Cormack


Ian H. Witten | Alistair Moffat | Timothy C. Bell
Managing
Compressing and Indexing Documents and Images
Gigabytes
SECOND EDITION

elastic

Resources

Links, links, links



Links

https://lucene.apache.org/core/8_2_0/core/org/apache/lucene/search/similarities/TFIDFSimilarity.html

https://www.elastic.co/blog/whats-new-in-lucene-8

https://www.elastic.co/blog/faster-retrieval-of-top-hits-in-elasticsearch-with-block-max-wand

https://speakerdeck.com/elastic/amusing-algorithms-and-data-structures

https://www.elastic.co/blog/index-sorting-elasticsearch-6-0

https://raft.github.io/

https://github.com/elastic/elasticsearch-formal-models

https://gist.github.com/spinscale/b62c8b357fae7db3f14b7d3127758951

Links - probabilistic data structures

https://github.com/addthis/stream-lib

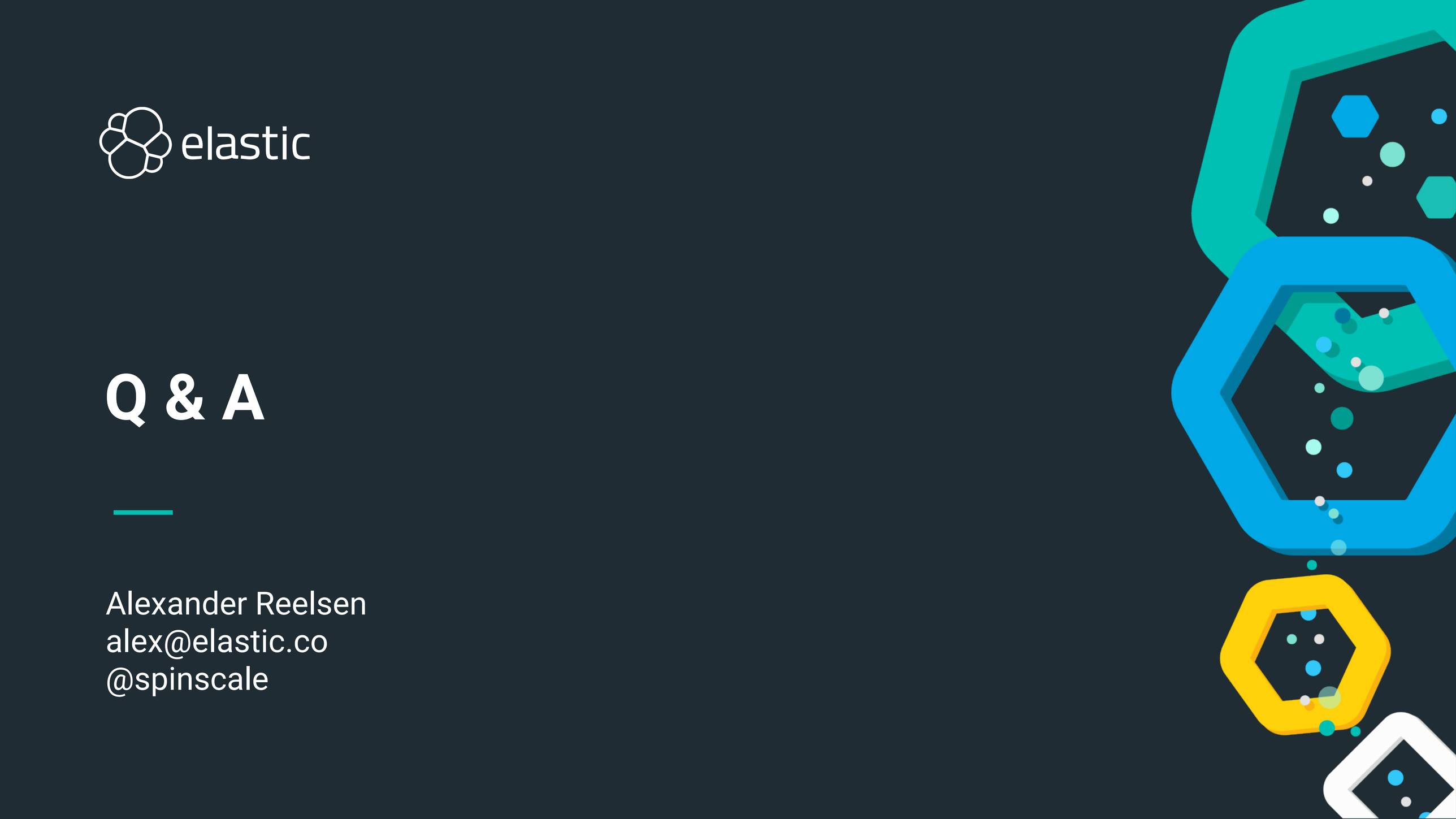
https://github.com/DataDog/sketches-java

https://github.com/HdrHistogram/HdrHistogram

https://github.com/JohnStarich/java-skip-list

https://github.com/addthis/stream-lib

https://static.googleusercontent.com/media/research.google.com/fr/pubs/archive/40671.pdf



Q & A

Alexander Reelsen
alex@elastic.co
@spinscale