Catch the Fraud

with Observability & Analytics

Philipp Krenn @xeraa

elastic

Developer 🥑

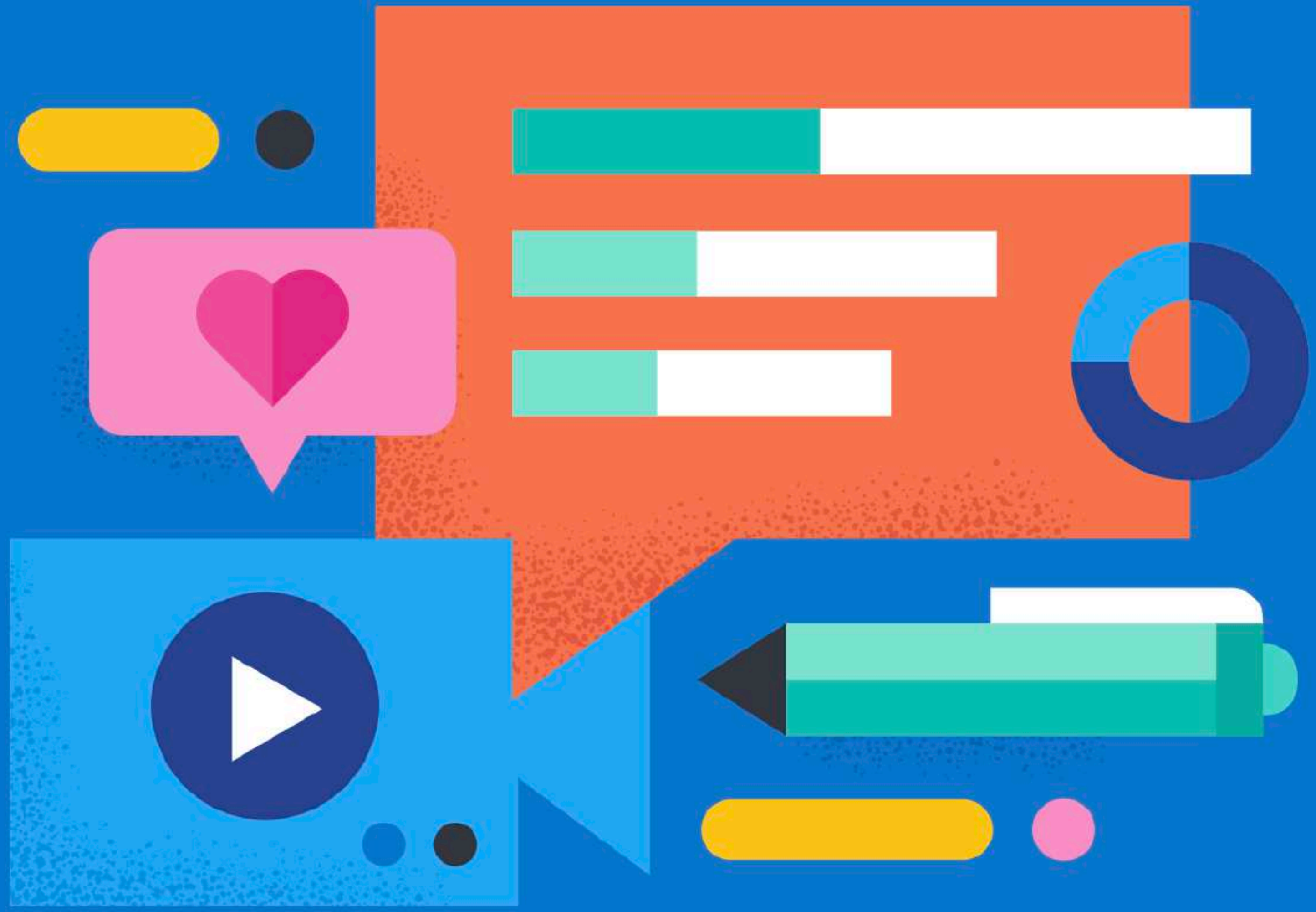
Community Contributors

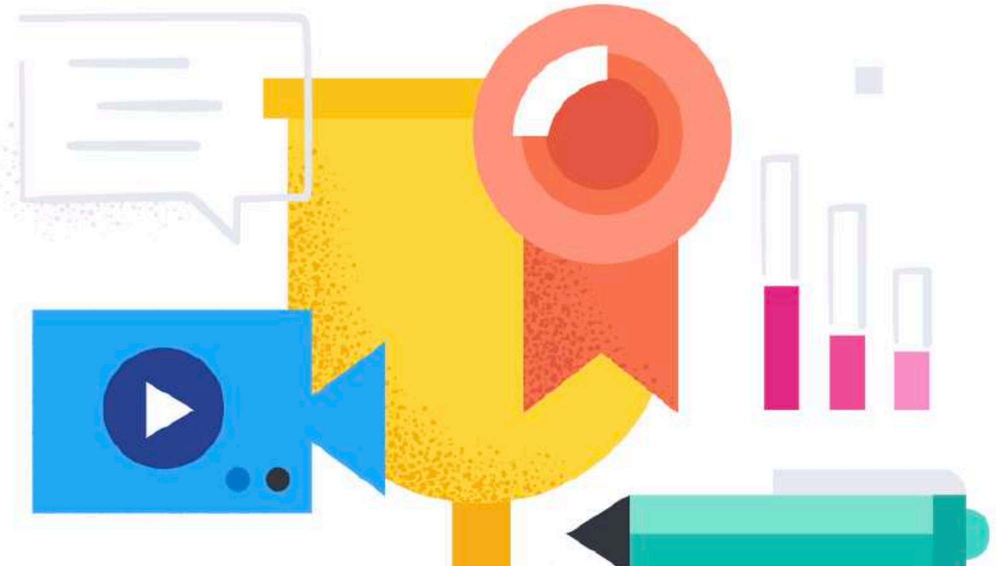
https://www.elastic.co/community/contributor

Elastic Contributor Program

We created the Elastic Contributor Program to recognize and reward the hard work of our awesome contributors, encourage knowledge sharing within the Elastic community, and build friendly competition around contributions.

Start contributing





How it works

Earn points by organizing events, presenting at events, writing content, recording videos, translating content, contributing code, answering technical questions, or validating others' contributions. At the end of the cycle top contributors will be rewarded with awesome Elastic prizes.

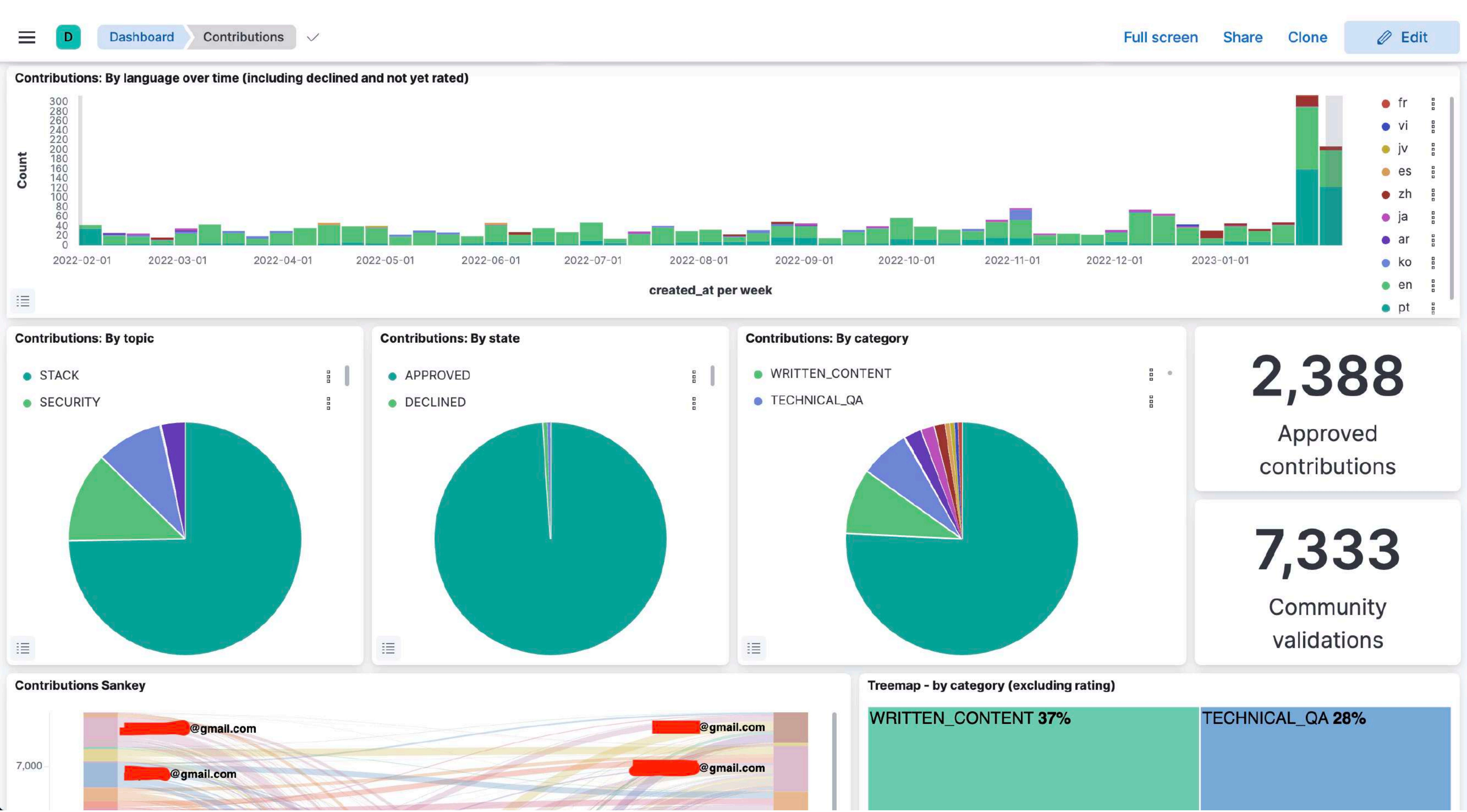
Contribution Type	Points awarded	Examples of contributions
Event organization	6 points	Meetup, hackathon, virtual event, or workshop
Presentation	6 points	Lecture, workshop, conference or meetup talks
Presentation slide deck	1 extra point	PDF, Powerpoint, or Google Slides
Written content	6 points	Article, blog post, or research paper
Share written content	1 extra point	Share the written content on your social media network
Code	2 or 6 points	Elastic GitHub repo: Bug reports (2 points), pull requests (6 points) Non-Elastic repos: demo (6 points) and projects using Elastic (6 points)
Video	4 points	Tutorial, podcasts, or use case overview
Translation	2 points	Translated Elastic blog posts

Demo

Kubernetes + Spring Boot / Data + Elasticsearch

Stats

Application + RUM + Tracing



Contributions: By language over time (including declined and not yet rated)

Contributions: By topic

Contributions: By state

Contributions: By category

2,388

Approved contributions

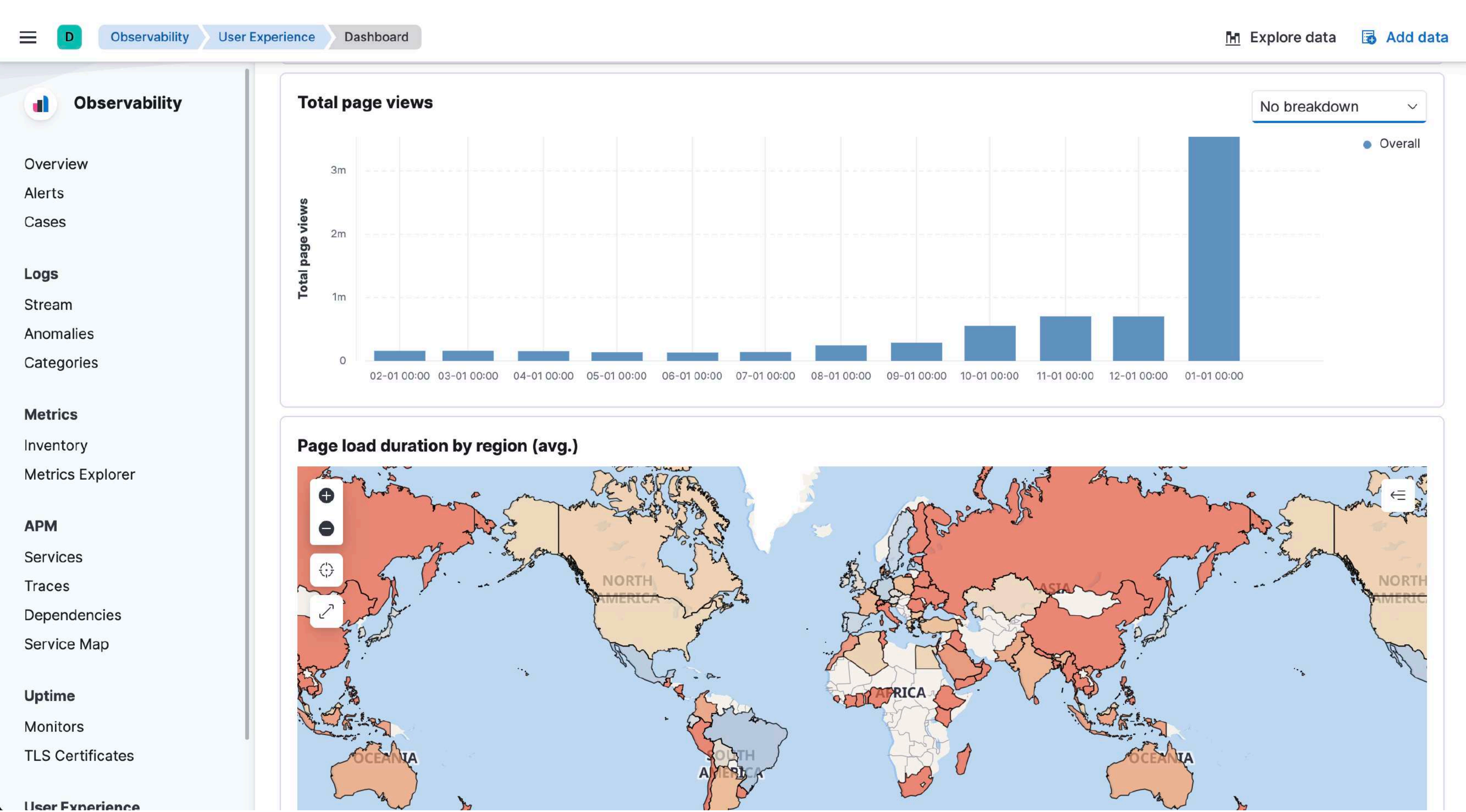
7,333

Community validations

Contributions Sankey

Treemap - by category (excluding rating)

You Can Win a 💻

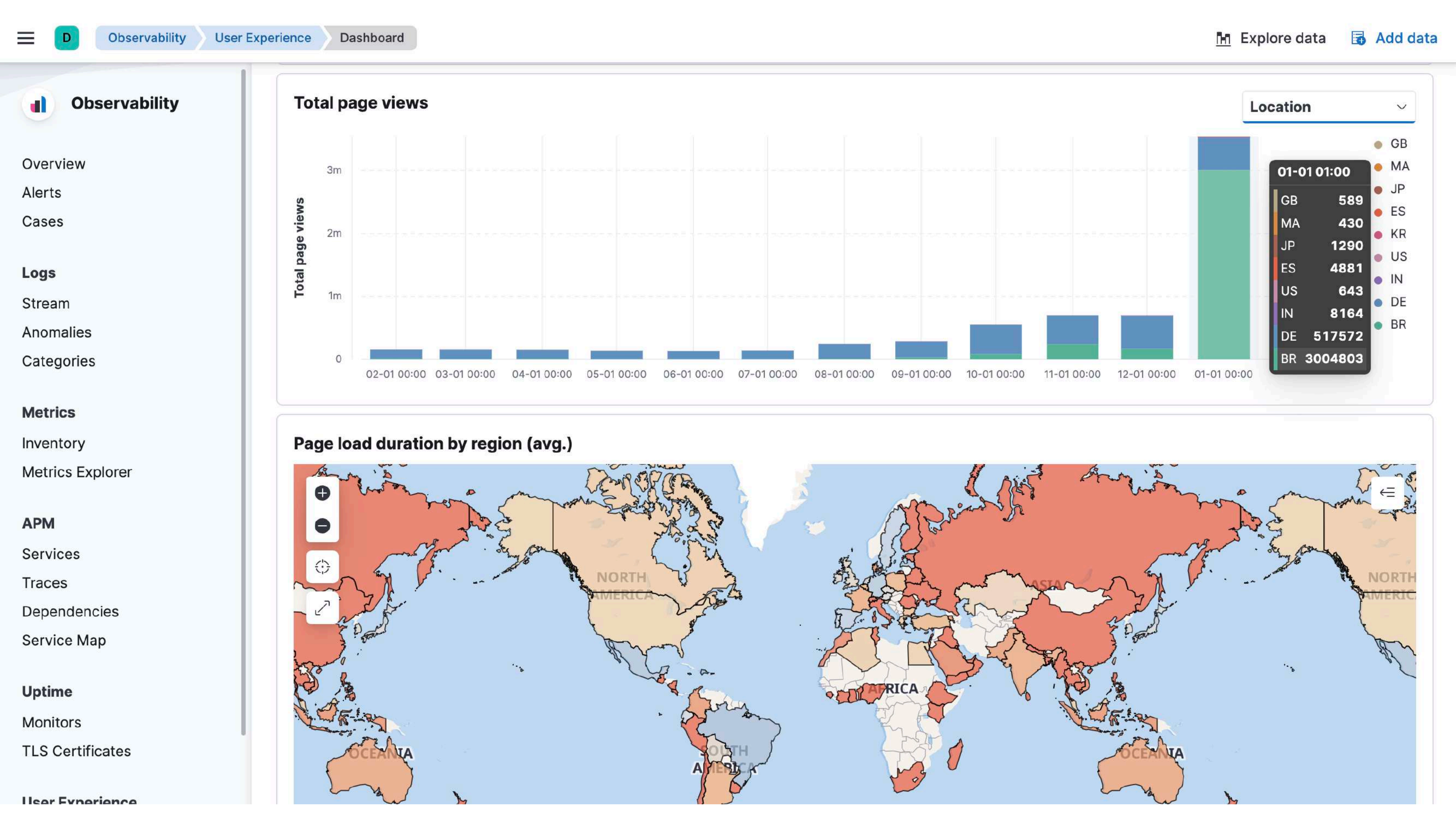


Total page views

Page load duration by region (avg.)

PAN AM
PA

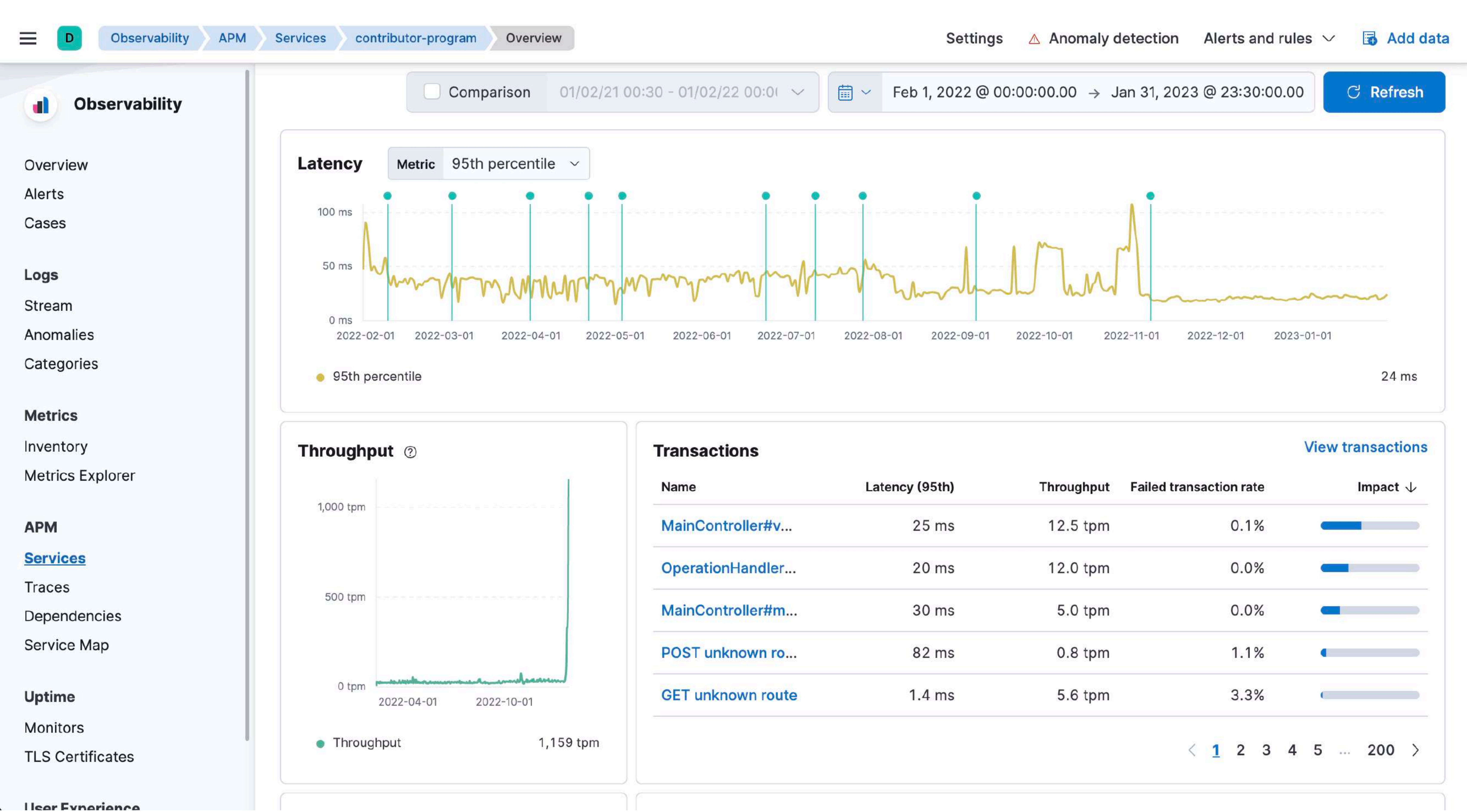
How to Cheat?



Total page views

01-01 01:00	
GB	589
MA	430
JP	1290
ES	4881
US	643
IN	8164
DE	517572
BR	3004803

Page load duration by region (avg.)



□ Comparison 01/02/21 00:30 - 01/02/22 00:0(

Feb 1, 2022 @ 00:00:00.00 → Jan 31, 2023 @ 23:30:00.00

Latency

Metric: 95th percentile

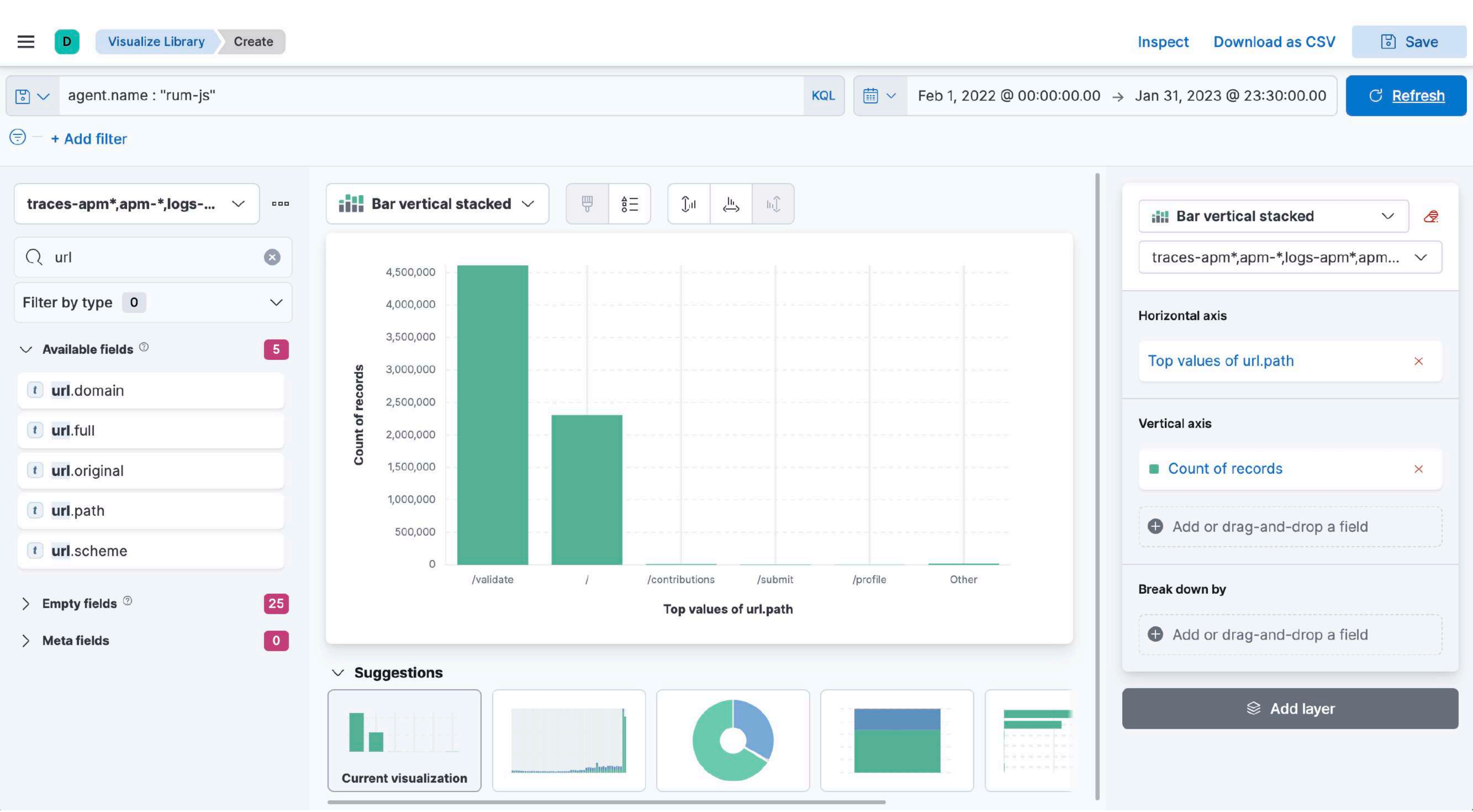
Throughput

Transactions

View transactions

Name	Latency (95th)	Throughput	Failed transaction rate	Impact ↓
MainController#v...	25 ms	12.5 tpm	0.1%	
OperationHandler...	20 ms	12.0 tpm	0.0%	
MainController#m...	30 ms	5.0 tpm	0.0%	
POST unknown ro...	82 ms	0.8 tpm	1.1%	
GET unknown route	1.4 ms	5.6 tpm	3.3%	

< 1 2 3 4 5 ... 200 >



agent.name : "rum-js"

Feb 1, 2022 @ 00:00:00.00 → Jan 31, 2023 @ 23:30:00.00

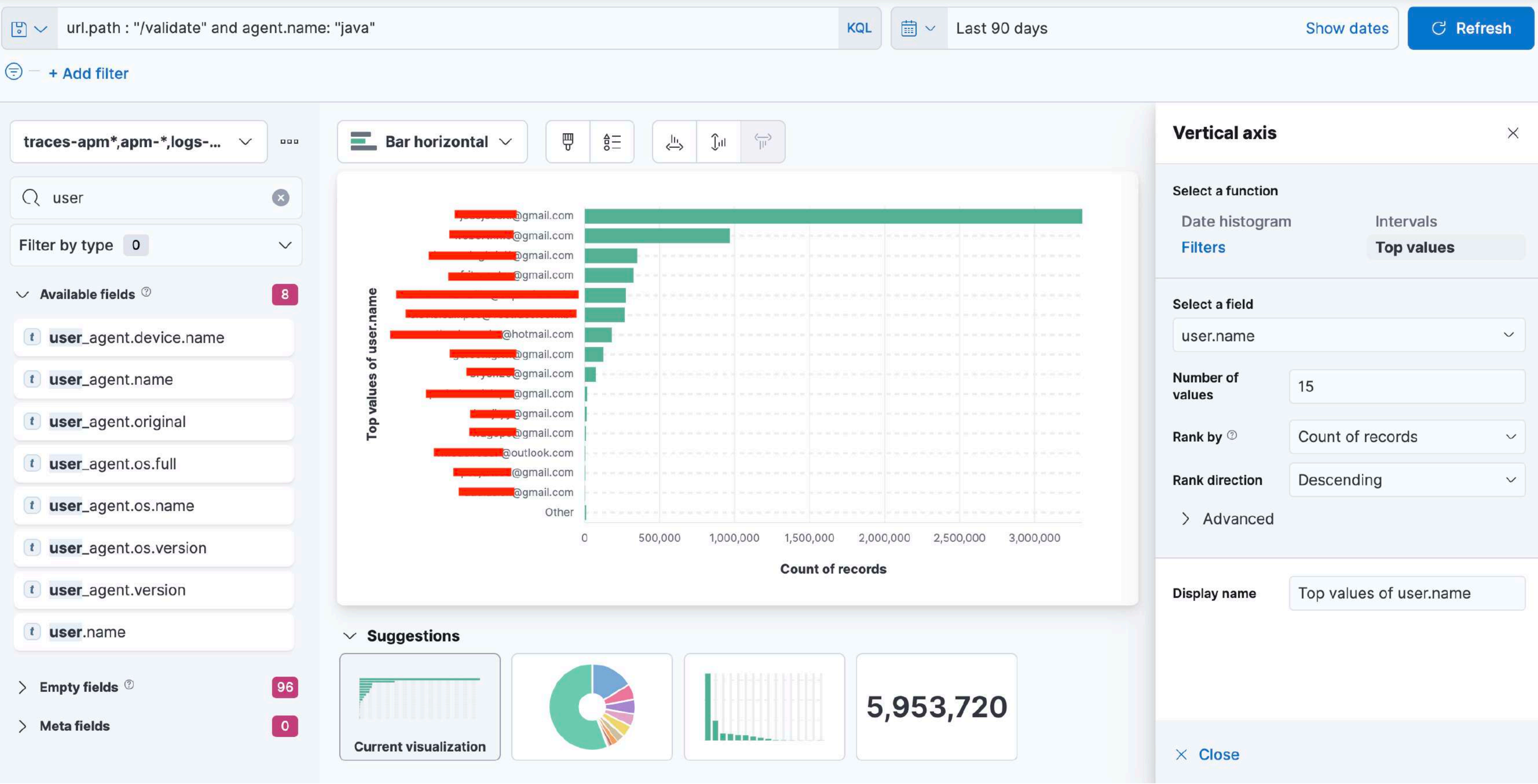
Bar vertical stacked

traces-apm*,apm-*,logs-apm*,apm...

Horizontal axis: Top values of url.path

Vertical axis: Count of records

Break down by: Add or drag-and-drop a field



url.path : "/validate" and agent.name: "java"

KQL

Last 90 days

Show dates

Refresh

+ Add filter

traces-apm*,apm-*,logs-...

user

Filter by type 0

Available fields 8

- user_agent.device.name
- user_agent.name
- user_agent.original
- user_agent.os.full
- user_agent.os.name
- user_agent.os.version
- user_agent.version
- user.name

Empty fields 96

Meta fields 0

Bar horizontal

Suggestions

Current visualization

5,953,720

Vertical axis

Select a function

Select a field: user.name

Number of values: 15

Rank by: Count of records

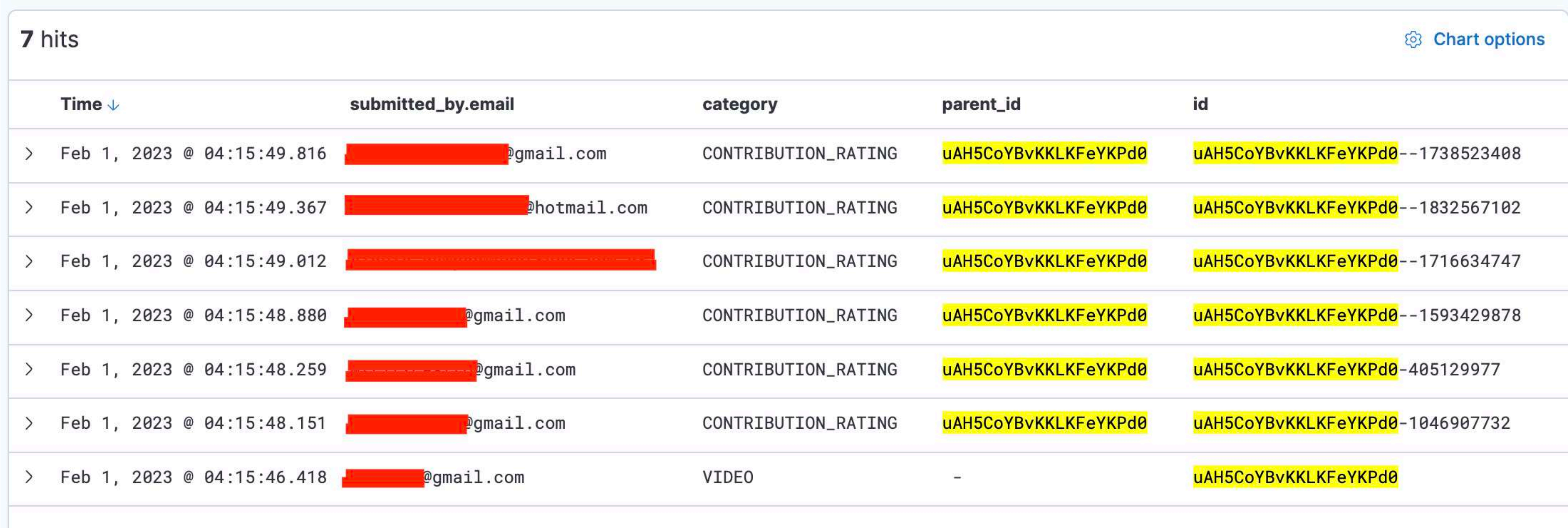
Rank direction: Descending

Advanced

Display name: Top values of user.name

Close

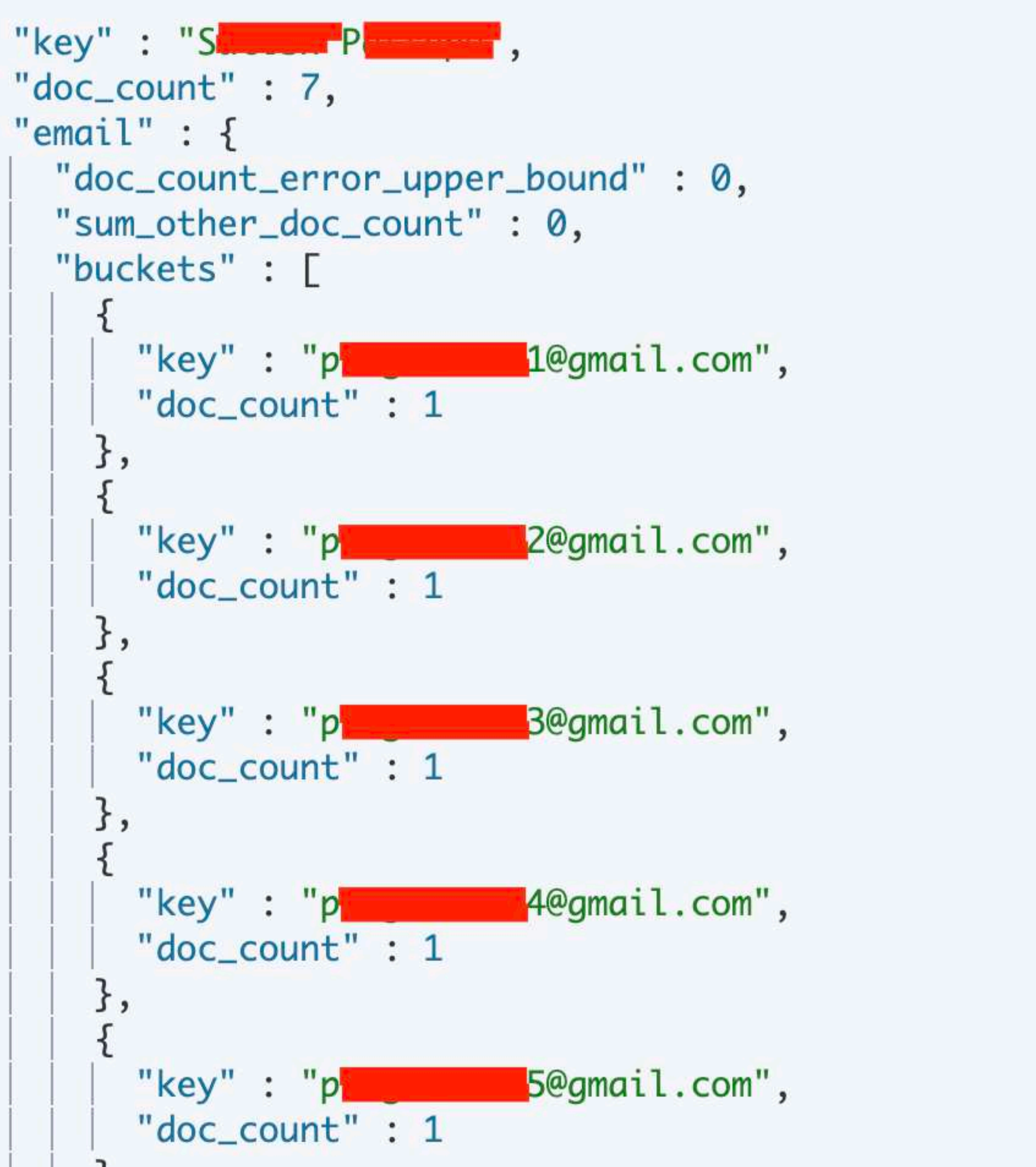
Timing



7 hits

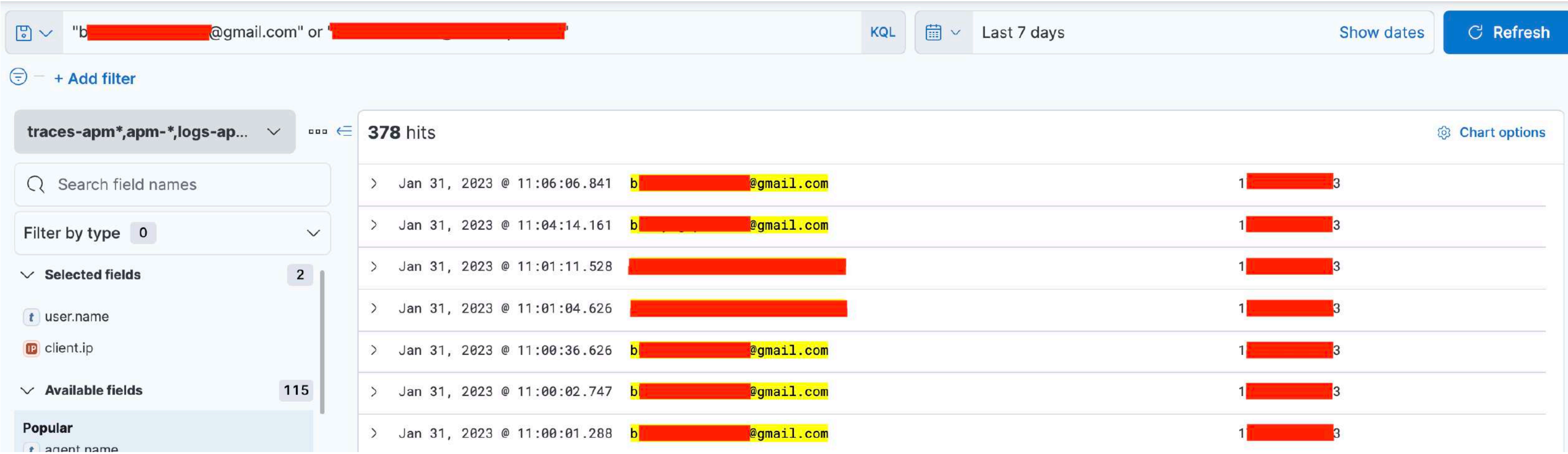
	Time ↓	submitted_by.email	category	parent_id	id
>	Feb 1, 2023 @ 04:15:49.816	[redacted]@gmail.com	CONTRIBUTION_RATING	uAH5CoYBvKKLKFeYKPd0	uAH5CoYBvKKLKFeYKPd0--1738523408
>	Feb 1, 2023 @ 04:15:49.367	[redacted]@hotmail.com	CONTRIBUTION_RATING	uAH5CoYBvKKLKFeYKPd0	uAH5CoYBvKKLKFeYKPd0--1832567102
>	Feb 1, 2023 @ 04:15:49.012	[redacted]	CONTRIBUTION_RATING	uAH5CoYBvKKLKFeYKPd0	uAH5CoYBvKKLKFeYKPd0--1716634747
>	Feb 1, 2023 @ 04:15:48.880	[redacted]@gmail.com	CONTRIBUTION_RATING	uAH5CoYBvKKLKFeYKPd0	uAH5CoYBvKKLKFeYKPd0--1593429878
>	Feb 1, 2023 @ 04:15:48.259	[redacted]@gmail.com	CONTRIBUTION_RATING	uAH5CoYBvKKLKFeYKPd0	uAH5CoYBvKKLKFeYKPd0-405129977
>	Feb 1, 2023 @ 04:15:48.151	[redacted]@gmail.com	CONTRIBUTION_RATING	uAH5CoYBvKKLKFeYKPd0	uAH5CoYBvKKLKFeYKPd0-1046907732
>	Feb 1, 2023 @ 04:15:46.418	[redacted]@gmail.com	VIDEO	-	uAH5CoYBvKKLKFeYKPd0

Names



```
"key" : "S[redacted]P[redacted]",
"doc_count" : 7,
"email" : {
  "doc_count_error_upper_bound" : 0,
  "sum_other_doc_count" : 0,
  "buckets" : [
    {
      "key" : "p[redacted]1@gmail.com",
      "doc_count" : 1
    },
    {
      "key" : "p[redacted]2@gmail.com",
      "doc_count" : 1
    },
    {
      "key" : "p[redacted]3@gmail.com",
      "doc_count" : 1
    },
    {
      "key" : "p[redacted]4@gmail.com",
      "doc_count" : 1
    },
    {
      "key" : "p[redacted]5@gmail.com",
      "doc_count" : 1
```

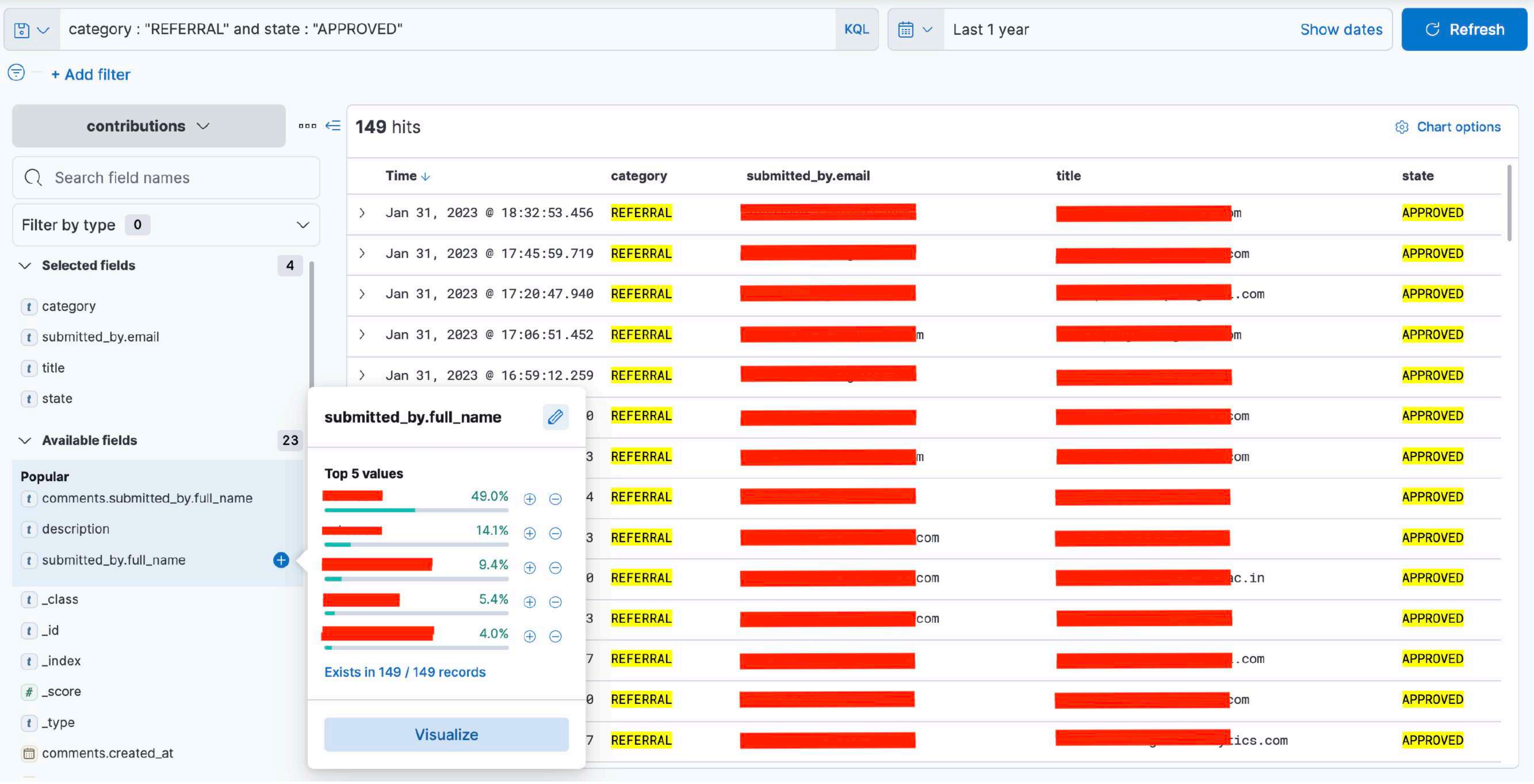
Multiple Accounts



"b[redacted]@gmail.com" or "[redacted]"

378 hits

```
Jan 31, 2023 @ 11:06:06.841   b[redacted]@gmail.com      1[redacted]3
Jan 31, 2023 @ 11:04:14.161   b[redacted]@gmail.com      1[redacted]3
Jan 31, 2023 @ 11:01:11.528   [redacted]                 1[redacted]3
Jan 31, 2023 @ 11:01:04.626   [redacted]                 1[redacted]3
Jan 31, 2023 @ 11:00:36.626   b[redacted]@gmail.com      1[redacted]3
Jan 31, 2023 @ 11:00:02.747   b[redacted]@gmail.com      1[redacted]3
Jan 31, 2023 @ 11:00:01.288   b[redacted]@gmail.com      1[redacted]3
```



Search field names

Filter by type 0

Selected fields 4
- category
- submitted_by.email
- title
- state

Available fields 23

Popular
- comments.submitted_by.full_name
- description
- submitted_by.full_name
- _class
- _id
- _index
- _score
- _type
- comments.created_at

149 hits

	Time ↓	category	submitted_by.email	title	state
›	Jan 31, 2023 @ 18:32:53.456	REFERRAL	[redacted]	[redacted]	APPROVED
›	Jan 31, 2023 @ 17:45:59.719	REFERRAL	[redacted]	[redacted]	APPROVED
›	Jan 31, 2023 @ 17:20:47.940	REFERRAL	[redacted]	[redacted]	APPROVED
›	Jan 31, 2023 @ 17:06:51.452	REFERRAL	[redacted]	[redacted]	APPROVED
›	Jan 31, 2023 @ 16:59:12.259	REFERRAL	[redacted]	[redacted]	APPROVED
	0	REFERRAL	[redacted]	[redacted]	APPROVED
	3	REFERRAL	[redacted]	[redacted]	APPROVED
	4	REFERRAL	[redacted]	[redacted]	APPROVED
	3	REFERRAL	[redacted]	[redacted]	APPROVED
	0	REFERRAL	[redacted]	[redacted]	APPROVED
	3	REFERRAL	[redacted]	[redacted]	APPROVED
	7	REFERRAL	[redacted]	[redacted]	APPROVED
	0	REFERRAL	[redacted]	[redacted]	APPROVED
	7	REFERRAL	[redacted]	[redacted]	APPROVED

submitted_by.full_name

Top 5 values

[redacted]	49.0%
[redacted]	14.1%
[redacted]	9.4%
[redacted]	5.4%
[redacted]	4.0%

Exists in 149 / 149 records

Reaction?

Conclusion

Work with the community

Be careful with incentives

Trust — but validate

Don't reveal your signals

Or change incentives

Catch the Fraud

with Observability & Analytics

Philipp Krenn @xeraa