elastic | The Search AI Company

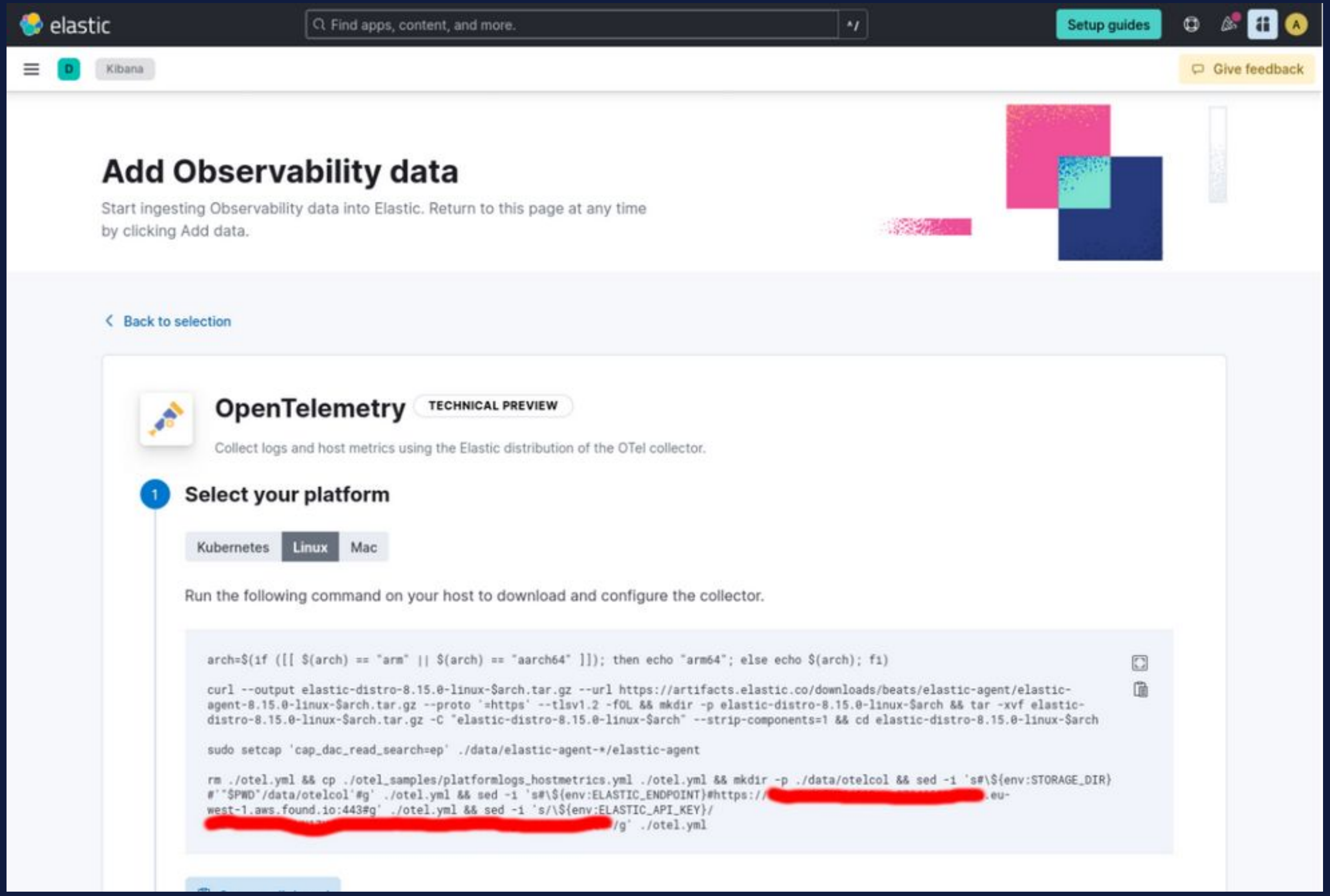
Observability with OTEK stack - OpenTelemetry, Elasticsearch, Kibana

Andrzej Stencel

Elastic Kraków Meetup, October 2024

DEMO:

Infrastructure monitoring with OpenTelemetry and Elasticsearch



Add Observability data

Start ingesting Observability data into Elastic. Return to this page at any time by clicking Add data.

< Back to selection

OpenTelemetry TECHNICAL PREVIEW

Collect logs and host metrics using the Elastic distribution of the OTel collector.

1 **Select your platform**

Kubernetes | **Linux** | Mac

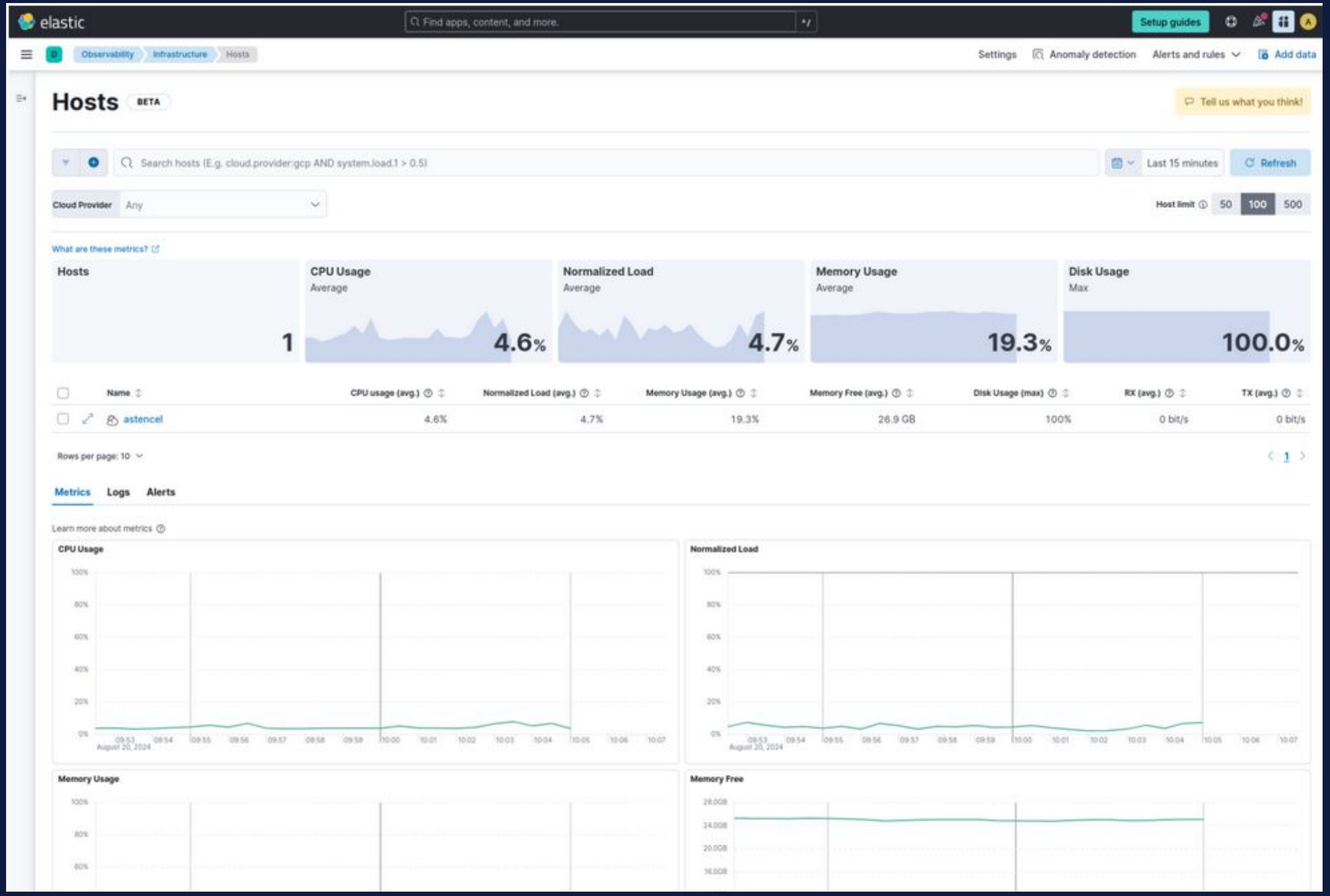
Run the following command on your host to download and configure the collector.

```
arch=$(if ([[ $(arch) == "arm" || $(arch) == "aarch64" ]]); then echo "arm64"; else echo $(arch); fi)

curl --output elastic-distro-8.15.0-linux-$arch.tar.gz --url https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-
agent-8.15.0-linux-$arch.tar.gz --proto '=https' --tlsv1.2 -fOL && mkdir -p elastic-distro-8.15.0-linux-$arch && tar -xvf elastic-
distro-8.15.0-linux-$arch.tar.gz -C "elastic-distro-8.15.0-linux-$arch" --strip-components=1 && cd elastic-distro-8.15.0-linux-$arch

sudo setcap 'cap_dac_read_search=ep' ./data/elastic-agent-*/elastic-agent

rm ./otel.yml && cp ./otel_samples/platformlogs_hostmetrics.yml ./otel.yml && mkdir -p ./data/otelcol && sed -i 's#\${env:STORAGE_DIR}
#'"$PWD"/data/otelcol'#g' ./otel.yml && sed -i 's#\${env:ELASTIC_ENDPOINT}#https://[redacted].eu-
west-1.aws.found.io:443#g' ./otel.yml && sed -i 's/\${env:ELASTIC_API_KEY}/
[redacted]/g' ./otel.yml
```



Hosts BETA

Hosts	CPU Usage Average	Normalized Load Average	Memory Usage Average	Disk Usage Max
1	4.6%	4.7%	19.3%	100.0%

Name	CPU usage (avg.)	Normalized Load (avg.)	Memory Usage (avg.)	Memory Free (avg.)	Disk Usage (max)	RX (avg.)	TX (avg.)
astencel	4.6%	4.7%	19.3%	26.9 GB	100%	0 bit/s	0 bit/s

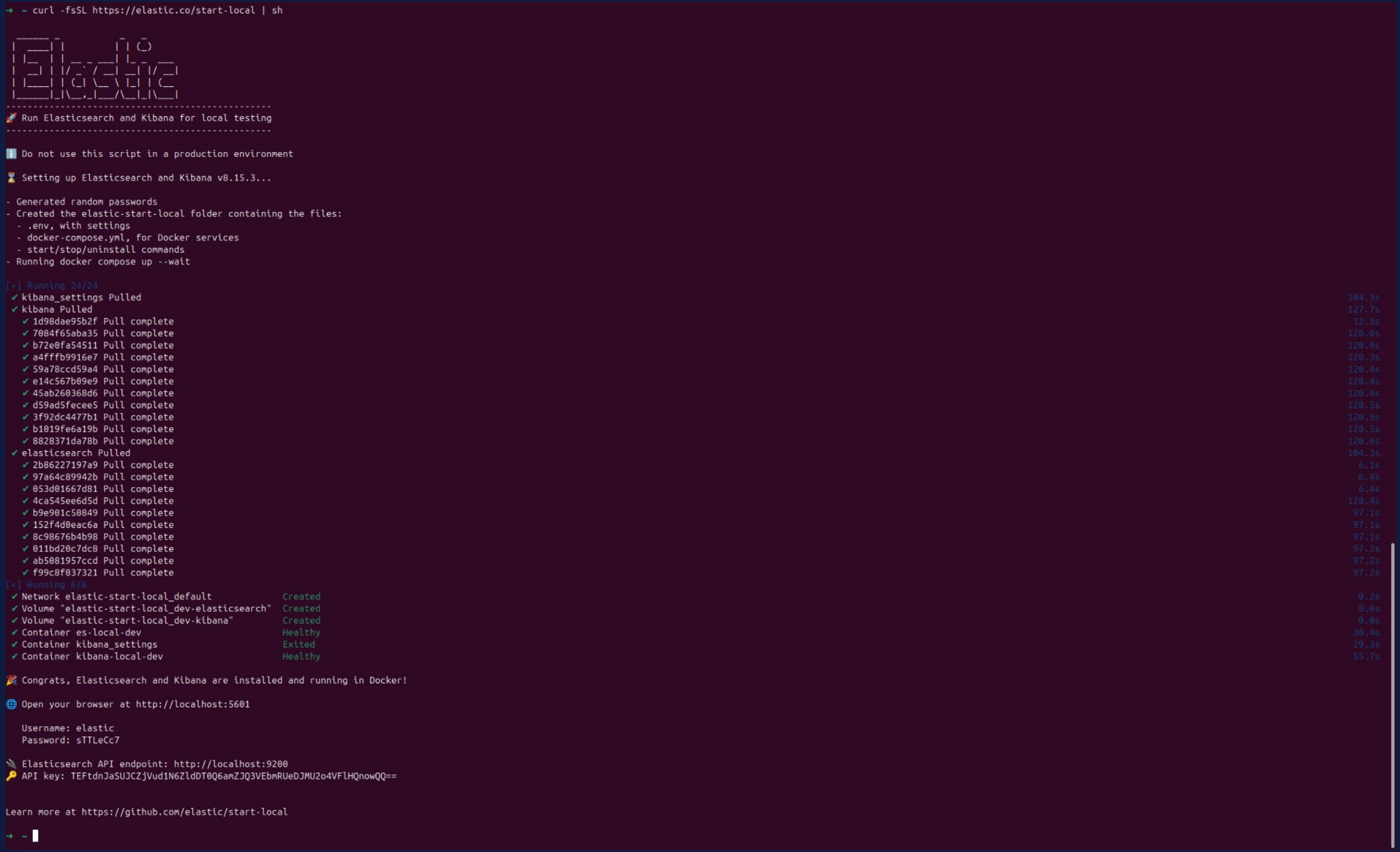
Rows per page: 10

Announcement: https://www.elastic.co/blog/whats-new-elastic-observability-8-15-0#introducing-the-elastic-distro-for-opentelemetry-collector

Walkthrough: https://andrzej-stencel.github.io/2024/08/28/elastic-distro-with-elastic-cloud.html

Start Elasticsearch and Kibana locally

$ curl -fsSL https://elastic.co/start-local | sh   Docs



```
→ ~ curl -fsSL https://elastic.co/start-local | sh

 ______ _           _   _
|  ____| |         | | (_)
| |__  | | __ _ ___| |_ _  ___
|  __| | |/ _` / __| __| |/ __|
| |____| | (_| \__ \ |_| | (__
|______|_|\__,_|___/\__|_|\___|
-------------------------------------------------
🚀 Run Elasticsearch and Kibana for local testing
-------------------------------------------------

ℹ️ Do not use this script in a production environment

⌛ Setting up Elasticsearch and Kibana v8.15.3...

- Generated random passwords
- Created the elastic-start-local folder containing the files:
  - .env, with settings
  - docker-compose.yml, for Docker services
  - start/stop/uninstall commands
- Running docker compose up --wait

[+] Running 24/24
 ✓ kibana_settings Pulled                                       104.3s
 ✓ kibana Pulled                                                127.7s
   ✓ 1d98dae95b2f Pull complete                                  12.3s
   ✓ 7084f65aba35 Pull complete                                 120.0s
   ✓ b72e0fa54511 Pull complete                                 120.0s
   ✓ a4fffb9916e7 Pull complete                                 120.3s
   ✓ 59a78ccd59a4 Pull complete                                 120.4s
   ✓ e14c567b09e9 Pull complete                                 120.4s
   ✓ 45ab260368d6 Pull complete                                 120.4s
   ✓ d59ad5fecee5 Pull complete                                 120.5s
   ✓ 3f92dc4477b1 Pull complete                                 120.5s
   ✓ b1019fe6a19b Pull complete                                 120.5s
   ✓ 8828371da78b Pull complete                                 120.6s
 ✓ elasticsearch Pulled                                         104.3s
   ✓ 2b86227197a9 Pull complete                                   6.1s
   ✓ 97a64c89942b Pull complete                                   6.4s
   ✓ 053d01667d81 Pull complete                                   6.4s
   ✓ 4ca545ee6d5d Pull complete                                 120.4s
   ✓ b9e901c50849 Pull complete                                  97.1s
   ✓ 152f4d0eac6a Pull complete                                  97.1s
   ✓ 8c98676b4b98 Pull complete                                  97.1s
   ✓ 011bd20c7dc8 Pull complete                                  97.2s
   ✓ ab5081957ccd Pull complete                                  97.2s
   ✓ f99c8f037321 Pull complete                                  97.2s
[+] Running 6/6
 ✓ Network elastic-start-local_default             Created        0.2s
 ✓ Volume "elastic-start-local_dev-elasticsearch"  Created        0.0s
 ✓ Volume "elastic-start-local_dev-kibana"         Created        0.0s
 ✓ Container es-local-dev                          Healthy       30.4s
 ✓ Container kibana_settings                       Exited        29.3s
 ✓ Container kibana-local-dev                      Healthy       55.7s

🎉 Congrats, Elasticsearch and Kibana are installed and running in Docker!

🌐 Open your browser at http://localhost:5601

   Username: elastic
   Password: sTTLeCc7

🔌 Elasticsearch API endpoint: http://localhost:9200
🔑 API key: TEFtdnJaSUJCZjVud1N6ZldDT0Q6amZJQ3VEbmRUeDJMU2o4VFlHQnowQQ==


Learn more at https://github.com/elastic/start-local

→ ~ ▌
```

Who am I?

Andrzej Stencel

Senior Software Engineer at Elastic

Maintainer of OpenTelemetry Collector Contrib

elastic

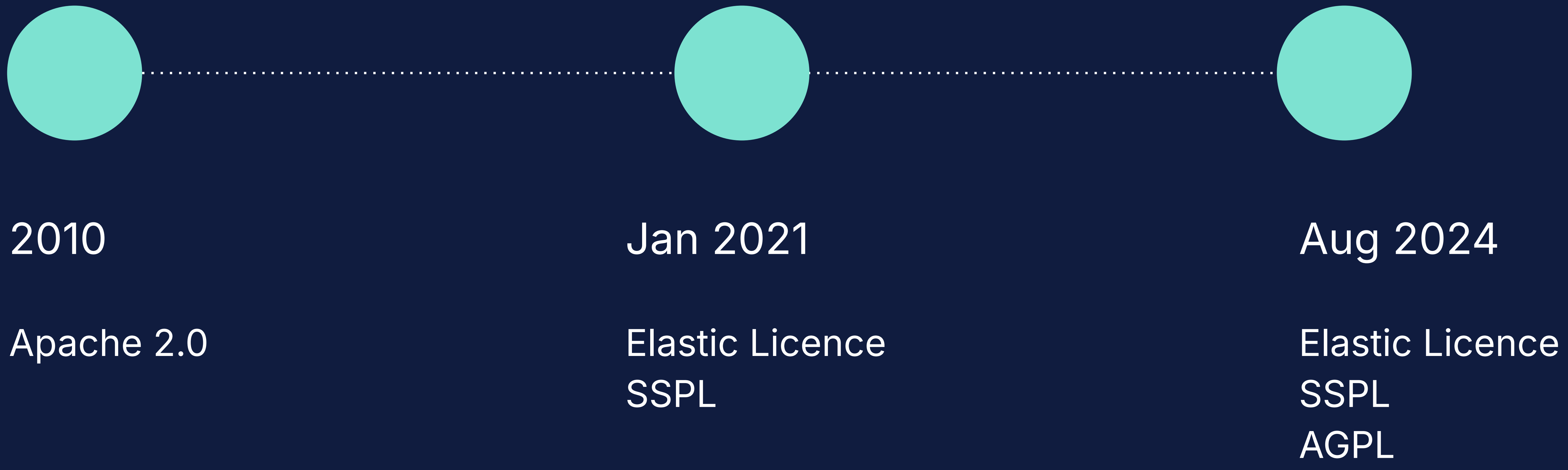
POLL:

Have you used OpenTelemetry Collector before?

In production?

🎉 Elasticsearch is open source again 🎉

https://www.elastic.co/blog/elasticsearch-is-open-source-again



2010

Apache 2.0

Jan 2021

Elastic Licence
SSPL

Aug 2024

Elastic Licence
SSPL
AGPL

Observability? What do you mean?

> Observability is the ability to understand the internal state of a system by examining its outputs. In the context of software, this means being able to understand the internal state of a system by examining its telemetry data, which includes traces, metrics, and logs.

OpenTelemetry docs

Why, why, why another agent?

- Logstash - can send an email 😲
- Beats - small and capable
- Elastic Agent - remotely managed
- OpenTelemetry Collector - ?...
  - not as capable as Logstash
  - not as small as Beats
  - remote management - in the works

OpenTelemetry - why?

- Vendor neutral specification, implementation
- Interoperability with standard protocol - OTLP
- Vendor-neutral telemetry with OTel semantic conventions
- Already rich, growing ecosystem
  - (auto-)instrumentation libraries
  - OpenTelemetry Operator
  - OpenTelemetry Kube Stack
  -

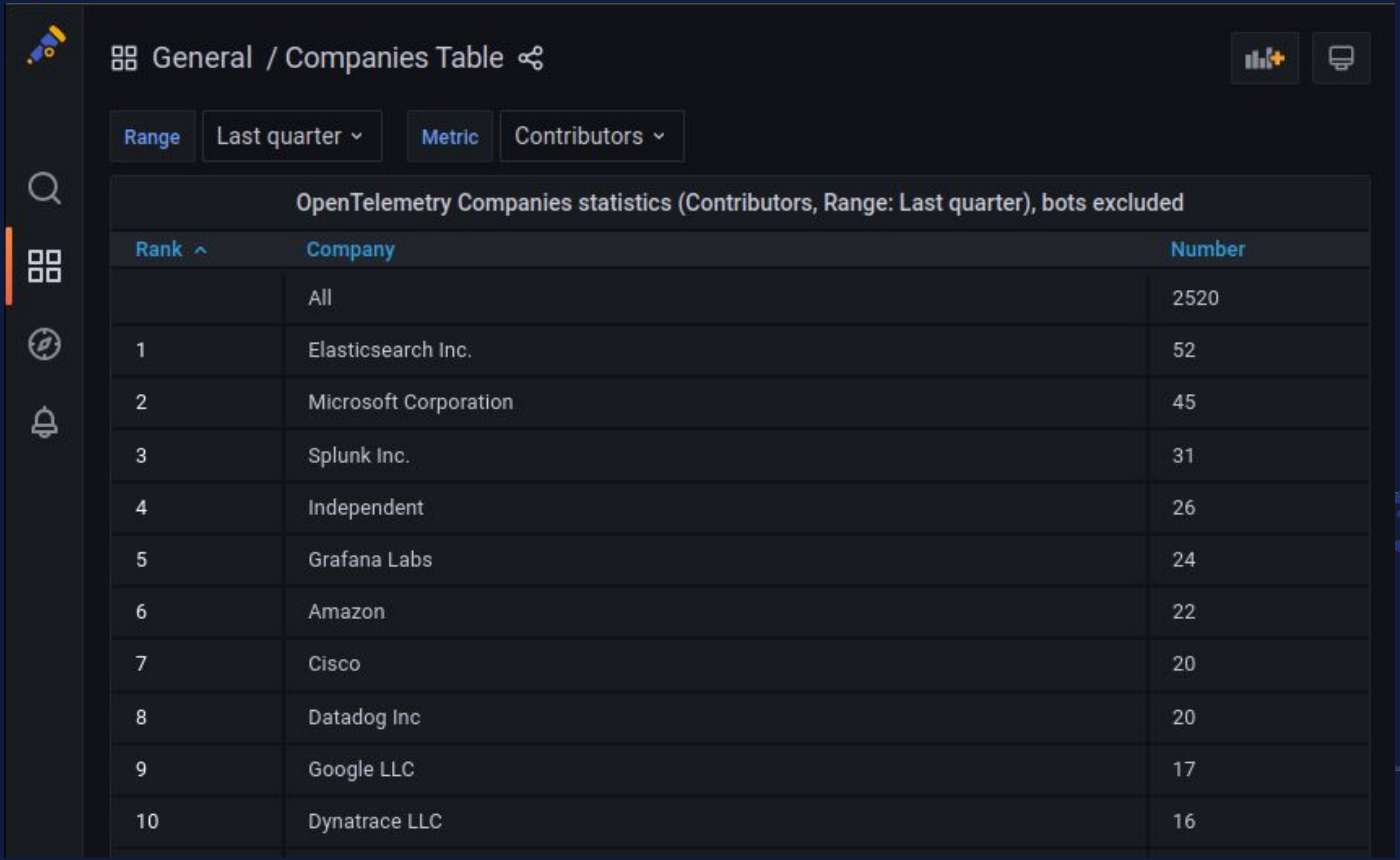
https://opentelemetry.io/docs/what-is-opentelemetry/#why-opentelemetry

Should you use OpenTelemetry today?

- You have an existing observability solution based on Logstash/Beats/Elastic Agent and it's meeting your needs
- You have an existing observability solution based on logs and metrics but it's not meeting your needs
- You are planning a new deployment of apps and/or observability solution
- ?

https://opentelemetry.io/status

Elastic currently has the most contributors to OpenTelemetry



Range: Last quarter

Metric: Contributors

OpenTelemetry Companies statistics (Contributors, Range: Last quarter), bots excluded

Rank	Company	Number
	All	2520
1	Elasticsearch Inc.	52
2	Microsoft Corporation	45
3	Splunk Inc.	31
4	Independent	26
5	Grafana Labs	24
6	Amazon	22
7	Cisco	20
8	Datadog Inc	20
9	Google LLC	17
10	Dynatrace LLC	16

DevStats

OpenTelemetry Collector:
File Log receiver

```
receivers:
  filelog:
    include:
      - /var/log/*.log
    exclude:
      - /var/log/kern.log
    start_at: end               # or “beginning”
    storage: file_storage
```

OpenTelemetry Collector:
Host Metrics receiver

```
receivers:
  hostmetrics:
    collection_interval: 10s
    scrapers:
      cpu:
        metrics:
          system.cpu.time:
            enabled: false
          system.cpu.utilization:
            enabled: true
```

OpenTelemetry Collector:
More receivers

- Core receivers: OTLP, Nop

- Contrib receivers

OpenTelemetry Collector:
Elasticsearch exporter

```yaml
exporters:
  elasticsearch:
    endpoint: "http://localhost:9200"
    api_key: ${env:ES_API_KEY}
    flush:
      interval: 1s
    mapping:
      mode: ecs
    logs_dynamic_index:
      enabled: true
    metrics_dynamic_index:
      enabled: true
    traces_dynamic_index:
      enabled: true
```

OpenTelemetry Collector: More exporters

- Core: OTLP, OTLP/HTTP, Nop, Debug

- Contrib exporters

OpenTelemetry Collector:
Debug exporter

```
exporters:
  debug:
    use_internal_logger: true
    verbosity: basic            # normal, detailed
```

Use `use_internal_logger: false` to:

- prevent sampling of exporter’s output
- prevent output from disappearing when `service::telemetry::log::level` is set to `warn` or `error`
- separate output from collector logs and redirect to a file with `> debug-output.txt`

OpenTelemetry Collector:
File Storage extension

```
extensions:
  file_storage:
    create_directory: true
    directory: ./otel-data
```

OpenTelemetry Collector: More extensions

- Core: zPages

- Contrib extensions

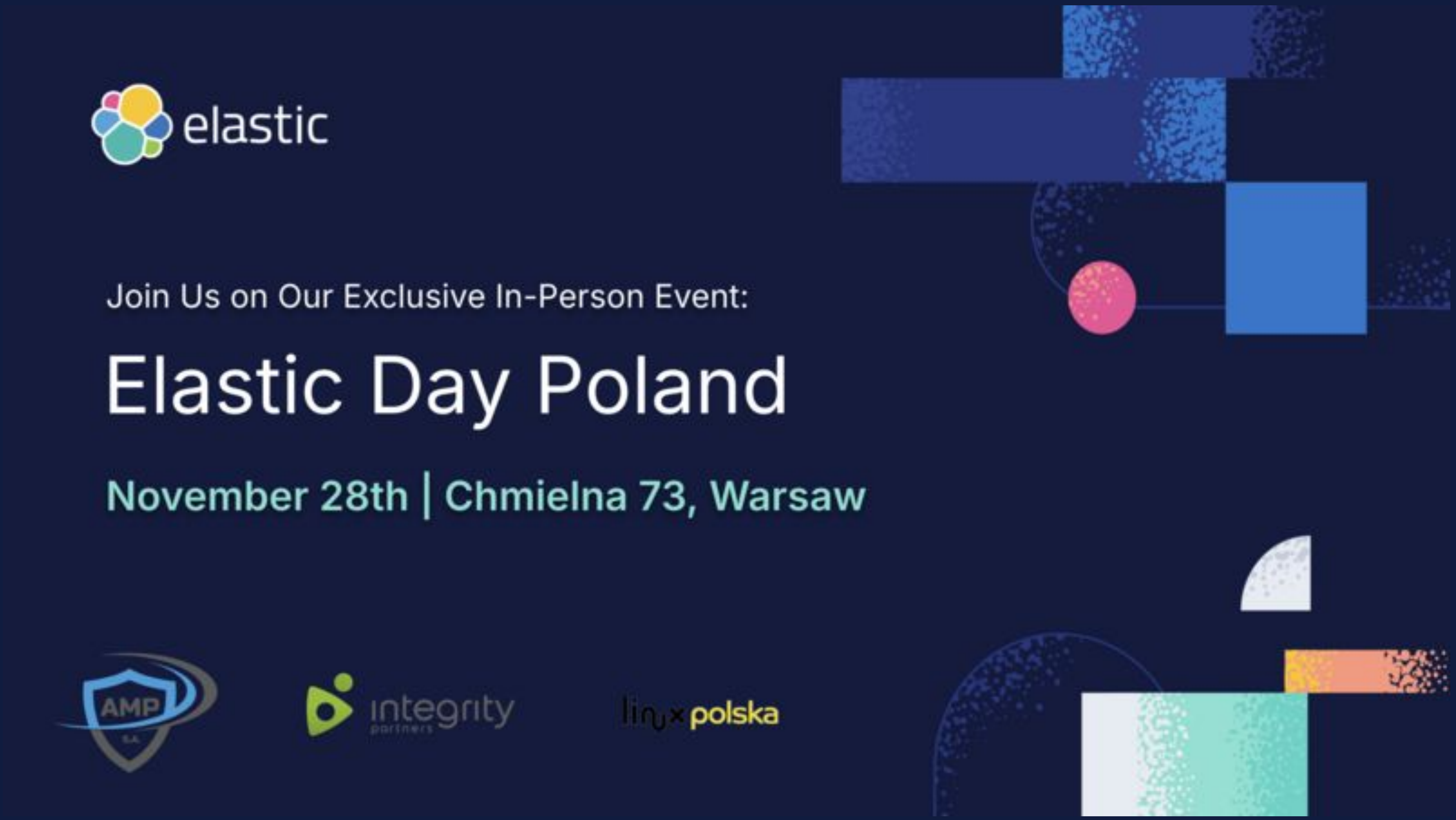
elastic

Bonus DEMO?

Collecting telemetry from workloads in Kubernetes with OpenTelemetry Operator

Join us for Elastic Day Poland!

https://events.elastic.co/elasticdaypoland



Join Us on Our Exclusive In-Person Event:

Elastic Day Poland

November 28th | Chmielna 73, Warsaw

- AI i Przyszłość Wyszukiwania
- AI i ML w Operacjach Bezpieczeństwa
- Elastic Observability
- Prezentacje Partnerów
- Możliwości Networkingu

Thank you!

Slides: https://andrzej-stencel.github.io/2024/10/21/elastic-krakow-meetup.html

elastic | The Search AI Company

Feedback: https://freesuggestionbox.com/pub/whqnnke