Embrace Observability

Timothy Mahoney
Ingka Group Digital (IKEA)
Splunk Observability Week 2023

About Me

- Timothy Mahoney
- American living in Sweden
- Former Satellite Network Engineer
- Volunteer Arbiter with RIPE NCC
- Vim user
- Really into obfuscated Awk

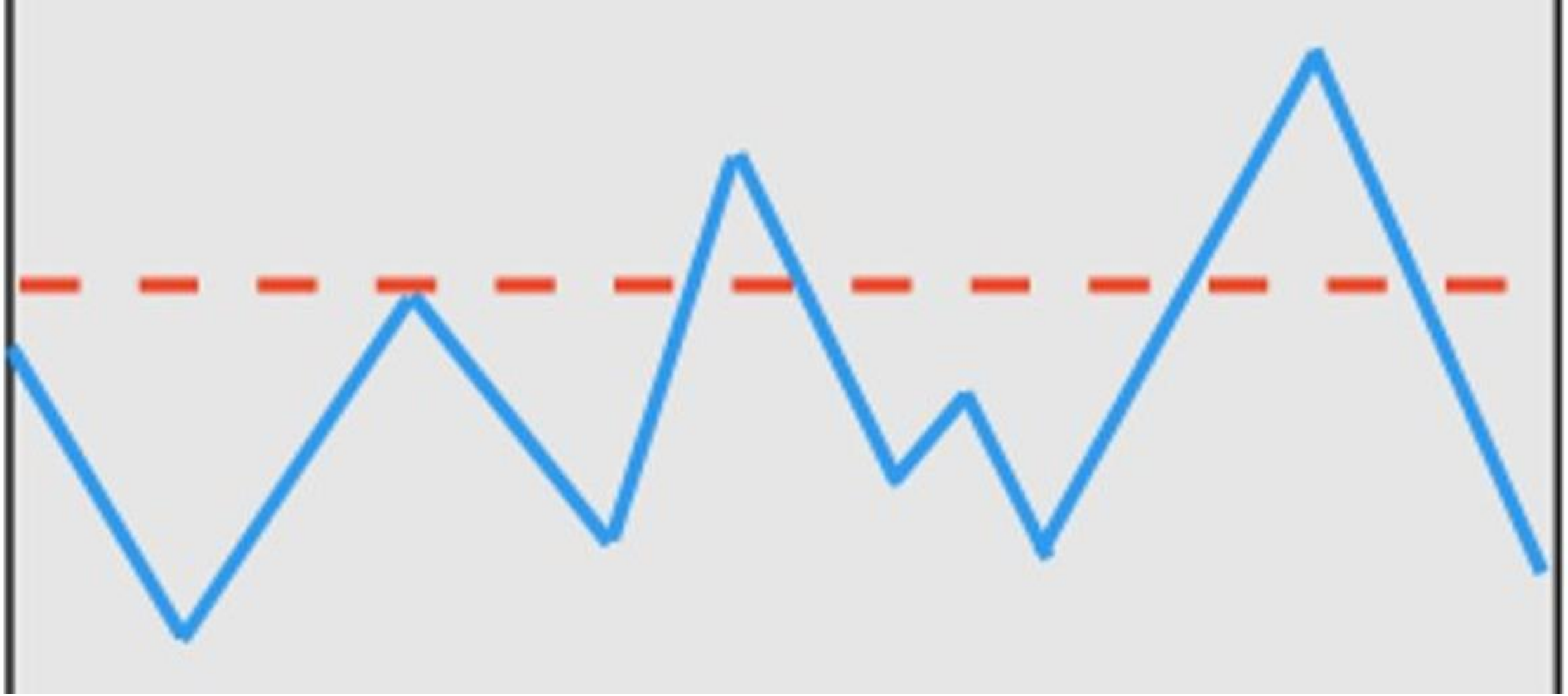
What I do

- Senior Systems Engineer in the Observability Pipeline Team
- Observability Framework
- OpenTelemetry and OpenTelemetry Collector
- Documentation, Examples, Demos, Labs, Tests
- INGKA Native Clouders program training lab on O11y and Distributed Tracing

What are we even talking about?

O11y in the IT systems context

- IT Operational Observability Signals
- The overused "Three Pillars of Observability"
- Different types of systems use different types of observability.



Metrics

IKEA

Metrics should be...

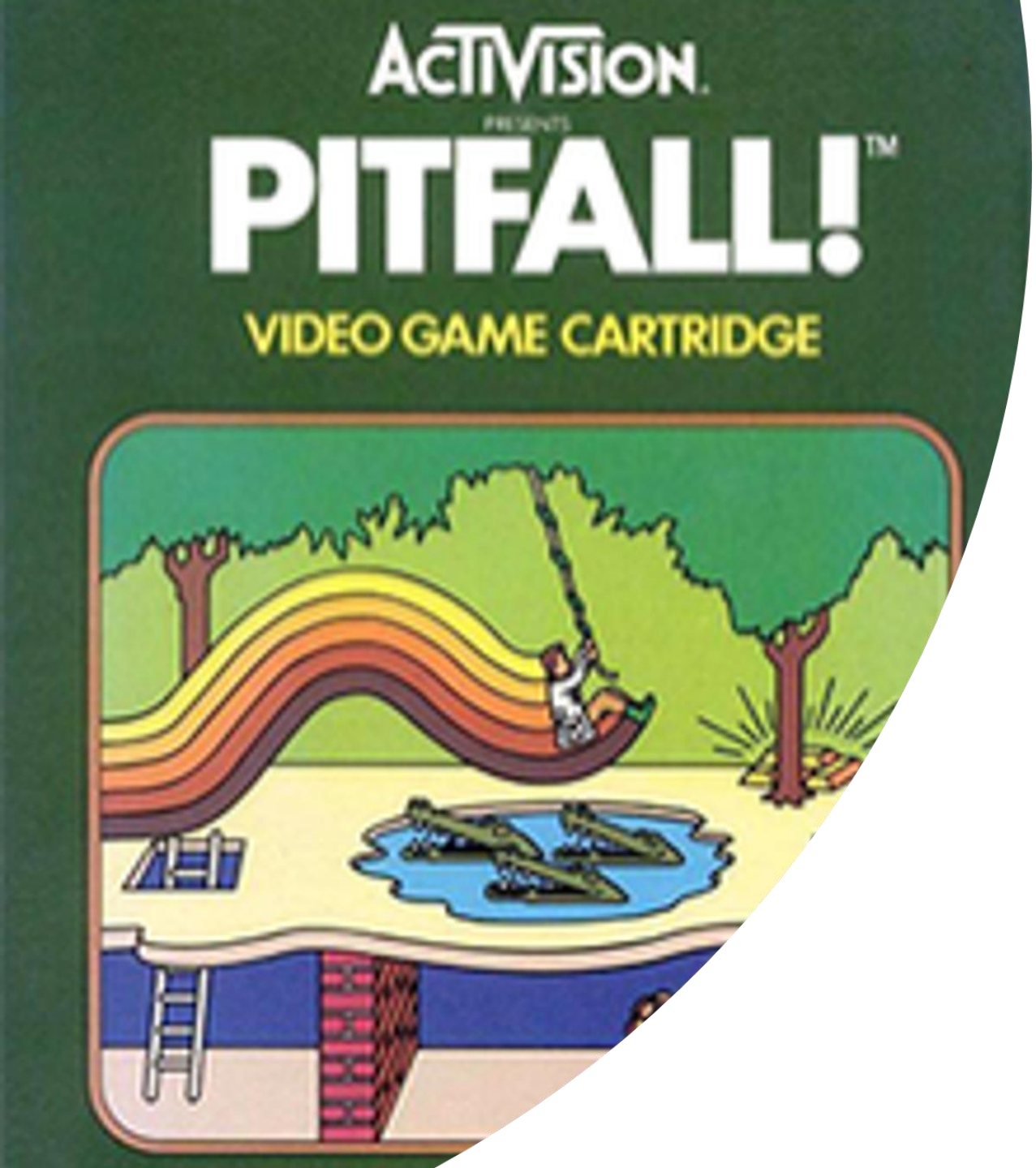
```
189.222.183.234 - - [05/Jun/2019:08:02:09 +0200] "GET /x.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:09 +0200] "GET /shell.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:10 +0200] "GET /htdocs.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:10 +0200] "GET /b.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:10 +0200] "GET /sane.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:10 +0200] "GET /desktop.ini.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:10 +0200] "GET /z.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:11 +0200] "GET /lala.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:11 +0200] "GET /lala-dpr.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:11 +0200] "GET /wpc.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:12 +0200] "GET /wpo.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:12 +0200] "GET /t6nv.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:12 +0200] "GET /muhstik.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:12 +0200] "GET /text.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:13 +0200] "GET /wp-config.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:13 +0200] "GET /muhstik.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:13 +0200] "GET /muhstik2.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:13 +0200] "GET /muhstiks.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:14 +0200] "GET /muhstik-dpr.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:14 +0200] "GET /lol.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:14 +0200] "GET /uploader.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:14 +0200] "GET /cmd.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:14 +0200] "GET /cmv.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:15 +0200] "GET /cmdd.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:15 +0200] "GET /knal.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:15 +0200] "GET /cmd.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:15 +0200] "GET /shell.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:16 +0200] "GET /appserv.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:16 +0200] "GET /scripts/setup.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:16 +0200] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:16 +0200] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:17 +0200] "GET /phpmyadmin/scripts/db___.init.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:17 +0200] "GET /phpMyAdmin/scripts/db___.init.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:17 +0200] "GET /plugins/weathermap/editor.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:17 +0200] "GET /cacti/plugins/weathermap/editor.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
189.222.183.234 - - [05/Jun/2019:08:02:17 +0200] "GET /index.php?s=%2f%69%6e%64%65%78%2f%5c%74%68%69%6e%6b%5c%61%70%70%2f%69%6e%76%6f%6b%65%66%75%6e%63%74%69%6f%6e&function=%63%61%6c%
189.222.183.234 - - [05/Jun/2019:08:02:18 +0200] "GET /d7.php HTTP/1.1" 301 185 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)" "-"
```

Logs

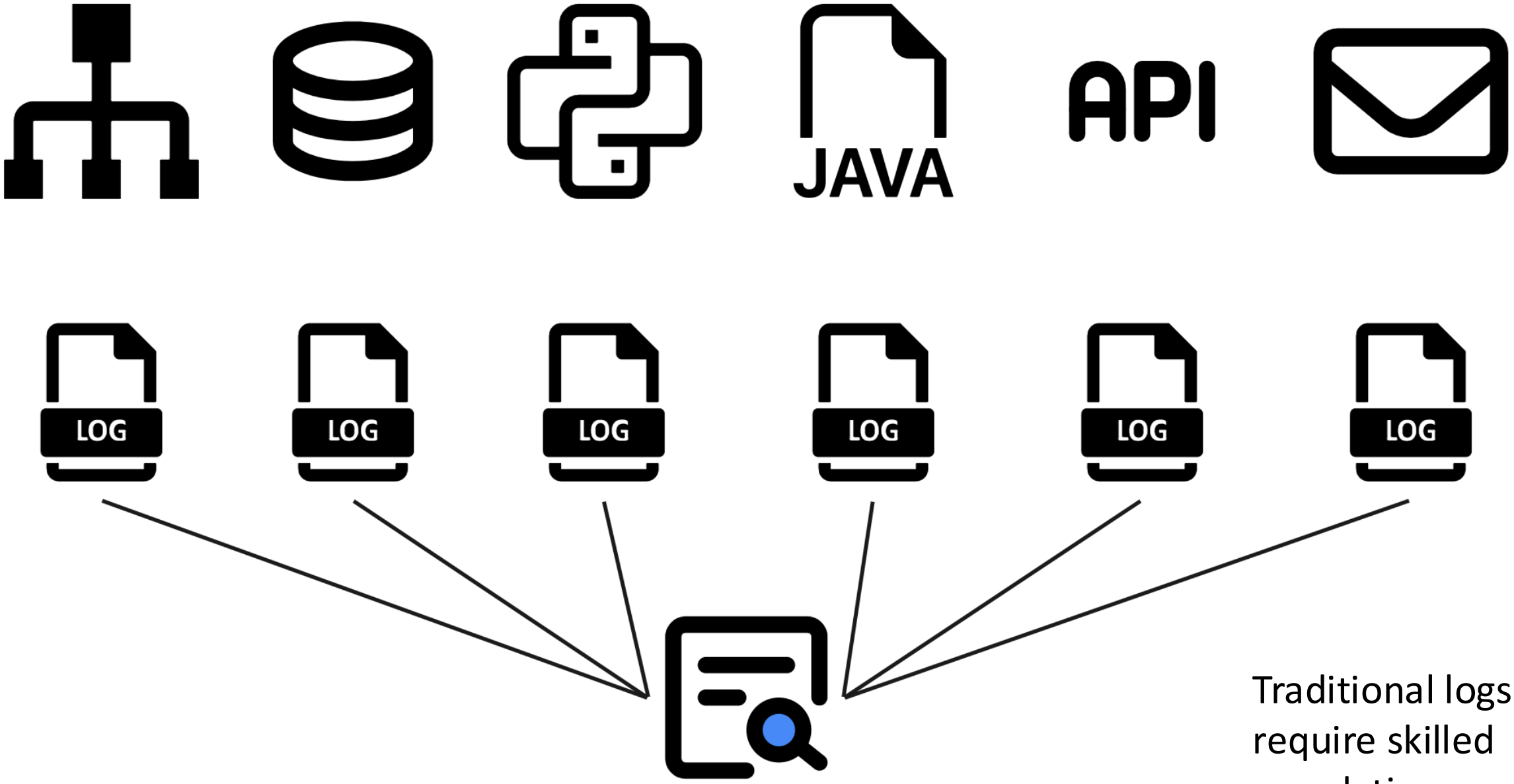
```
{
  "Timestamp": 1586960586000, // JSON needs to make a decision about
                              // how to represent nanoseconds.
  "Attributes": {
    "http.status_code": 500,
    "http.url": "http://example.com",
    "my.custom.application.tag": "hello",
  },
  "Resource": {
    "service.name": "donut_shop",
    "service.version": "semver:2.0.0",
    "k8s.pod.uid": "1138528c-c36e-11e9-a1a7-42010a800198",
  },
  "TraceId": "f4dbb3edd765f620", // this is a byte sequence
                                // (hex-encoded in JSON)
  "SpanId": "43222c2d51a7abe3",
  "SeverityText": "INFO",
  "SeverityNumber": 9,
  "Body": "20200415T072306-0700 INFO I like donuts"
}
```

```
  "bottles"
],
"@event" : {
  "timestamp" : 1553456417940,
  "logger" : "ExampleService.335",
  "line" : 339,
  "datetime" : "2019-03-24T19:40:17.940Z[UTC]",
  "thread" : {
    "id" : 1,
    "name" : "main"
  },
  "class" : "f48ebb70",
  "file" : "ExampleService.scala",
  "level" : "trace"
},
"just_an_arg" : "example",
"@message" : "Argument: justAnArg=example, another arg: ju
```

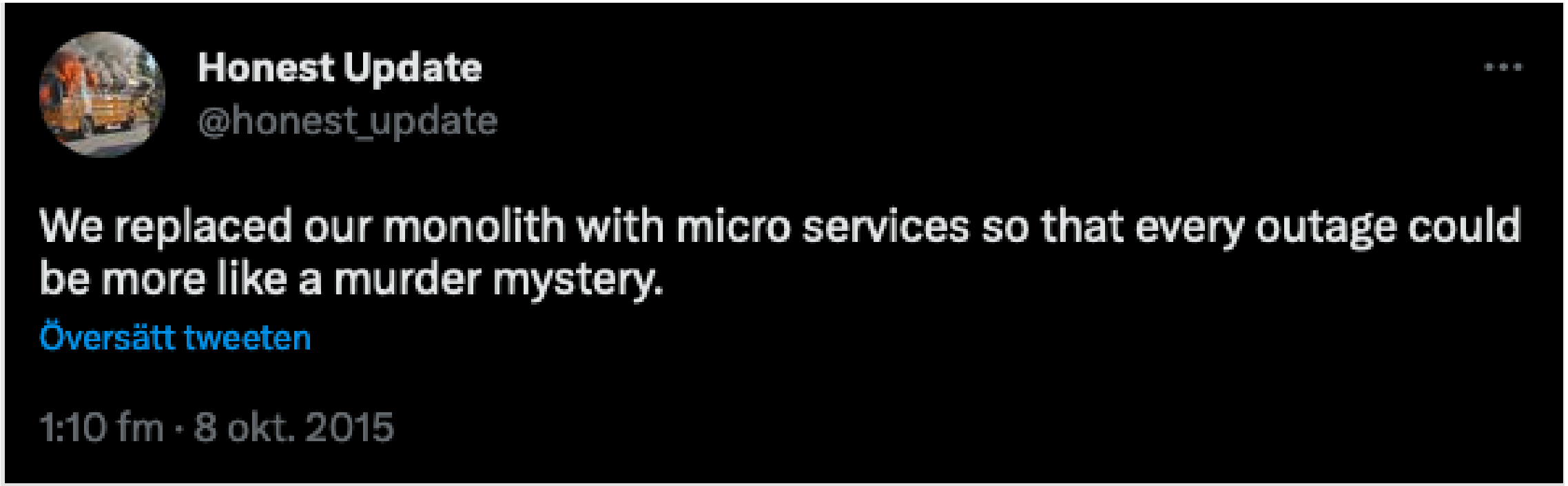
Making logs great again:



Pitfalls of logging

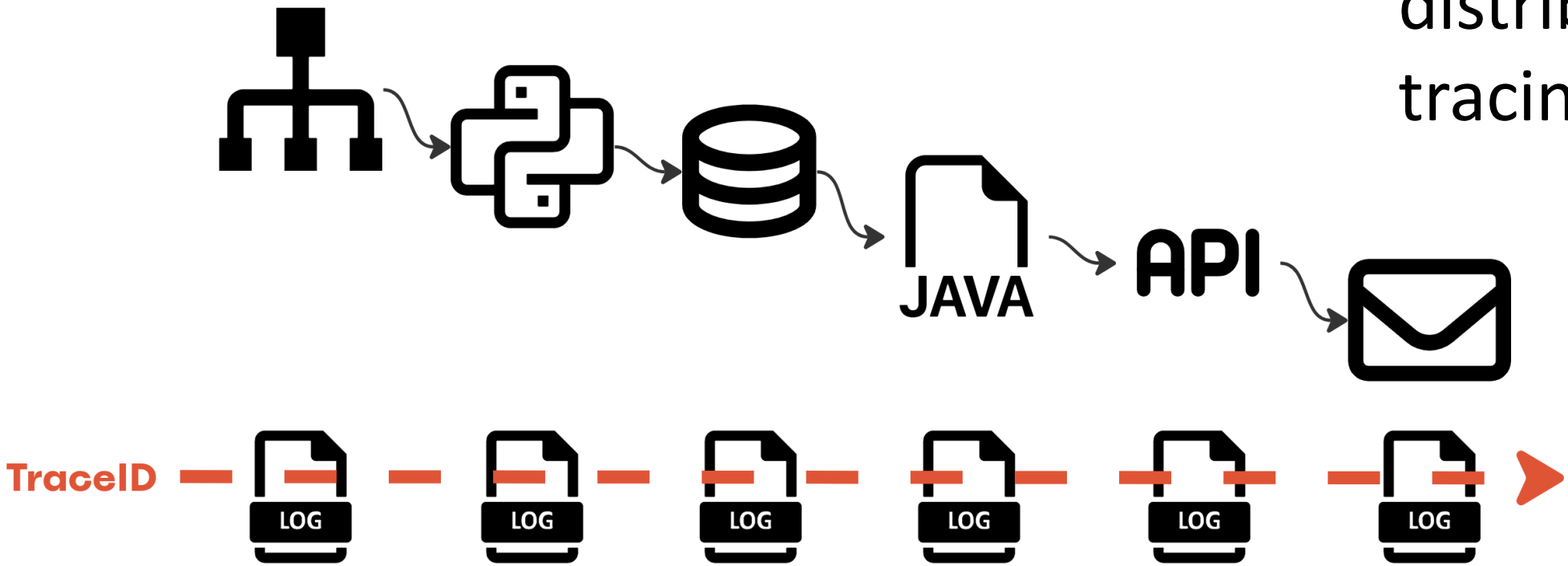


Traditional logs require skilled correlation.

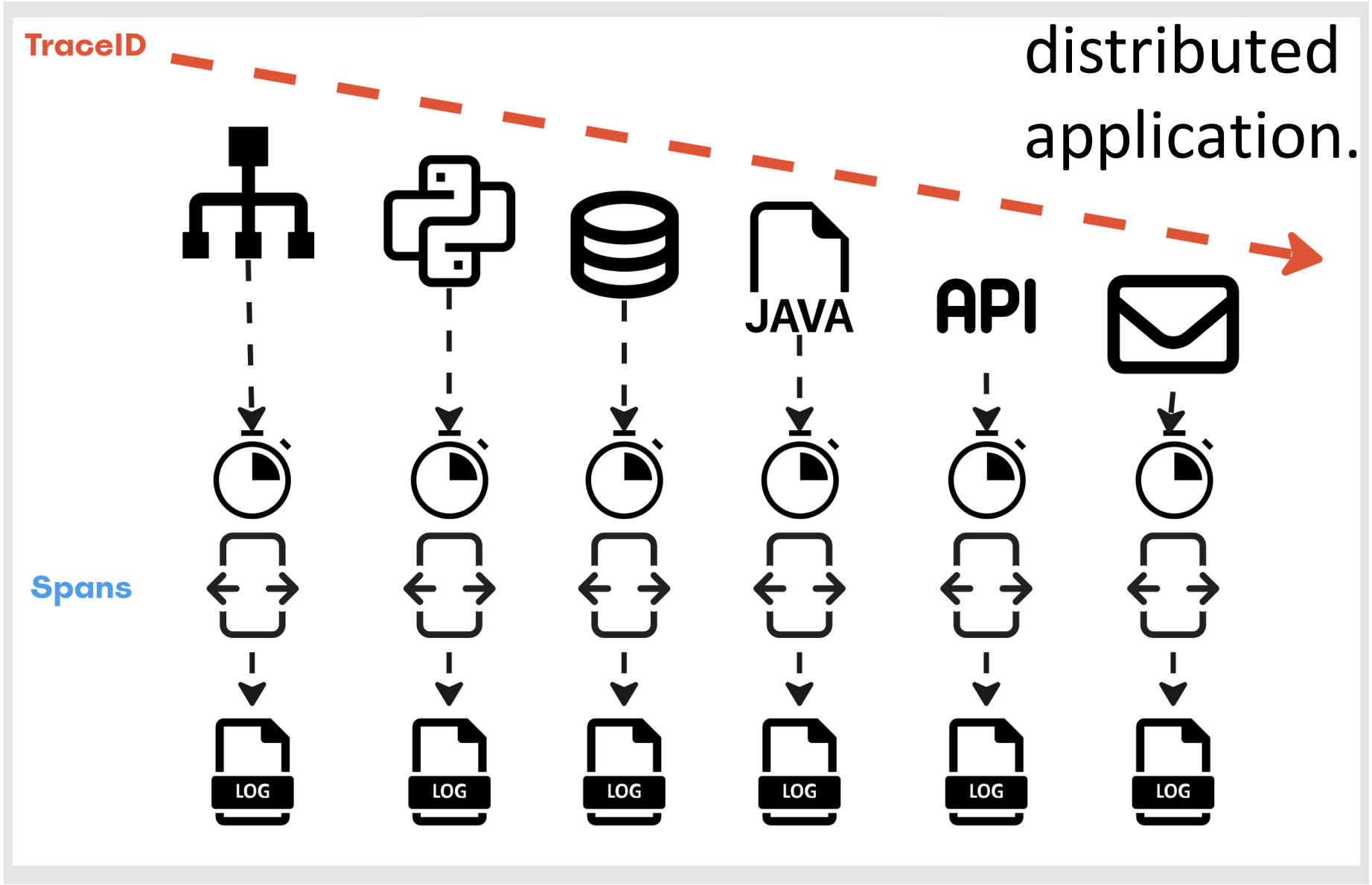


https://twitter.com/honest_update/status/651897353889259520?s=20

Enter distributed tracing



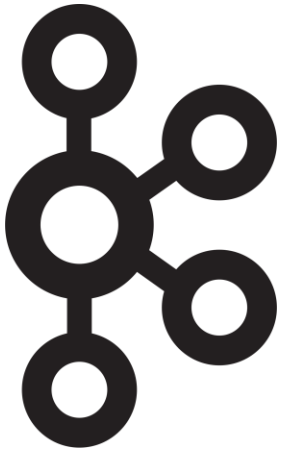
Tracing a distributed application.

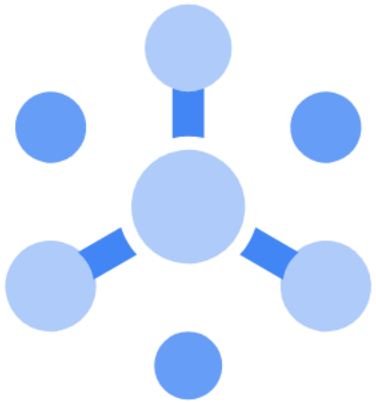


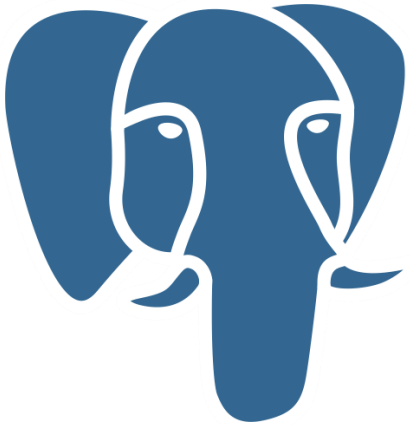
"We're just going to turn the logs off..."


```
  "events": [
    {
      "name": "",
      "message": "OK",
      "timestamp": "2021-10-22 16:04:01.209512872 +0000 UTC"
    }
  ]
}
```

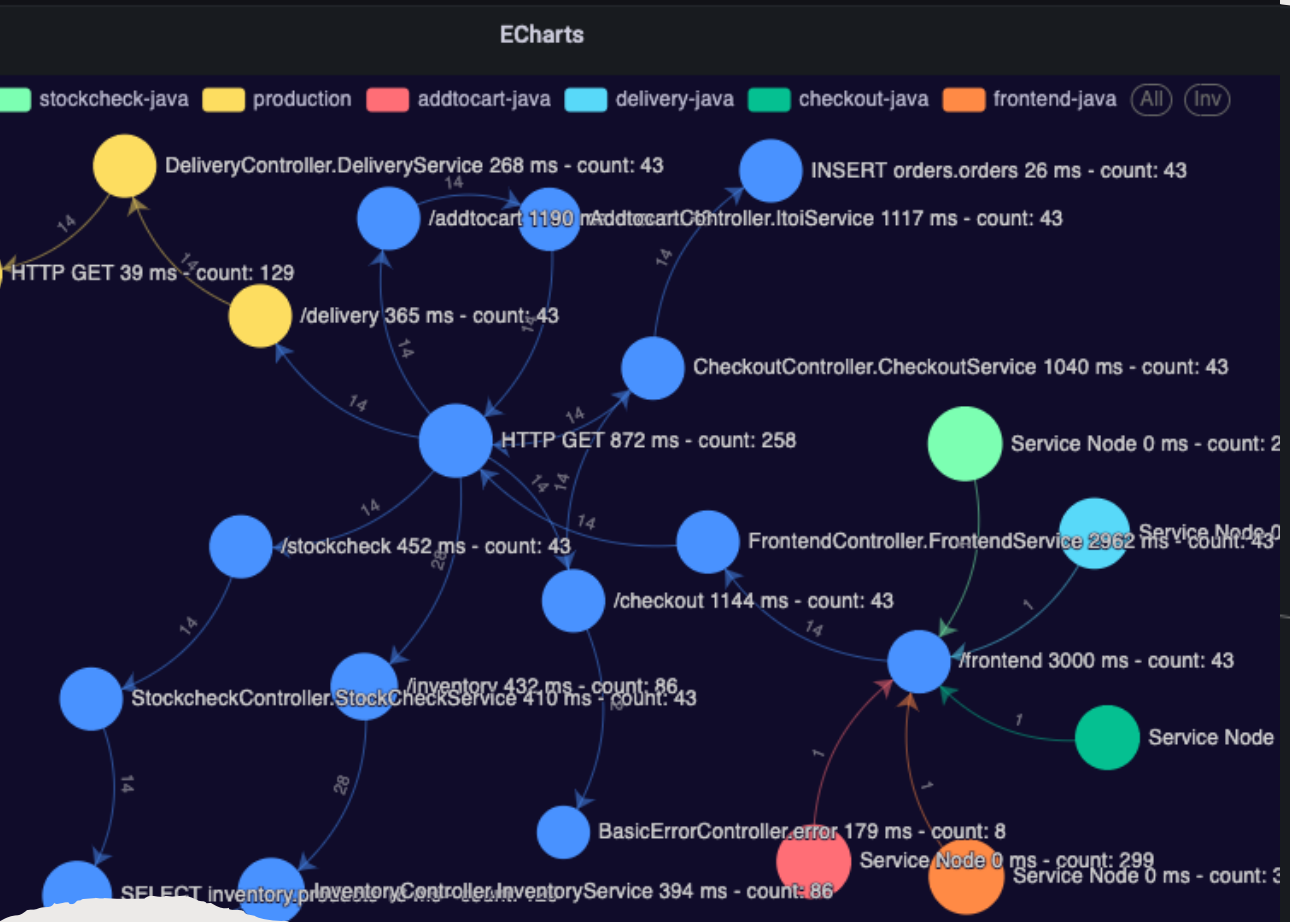

Trace propagation, message queues and databases.



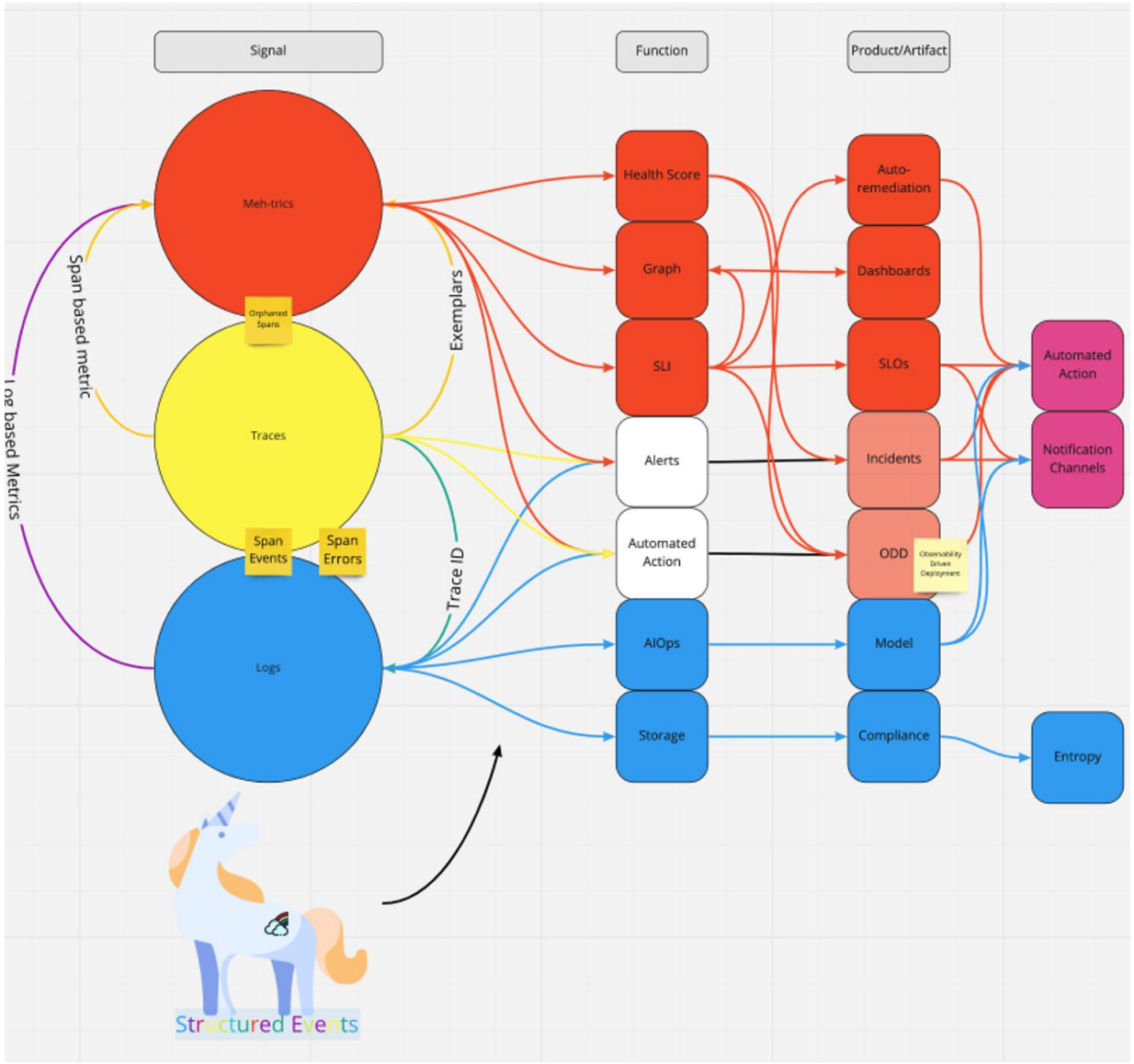




Tracing for CI/CD Pipelines



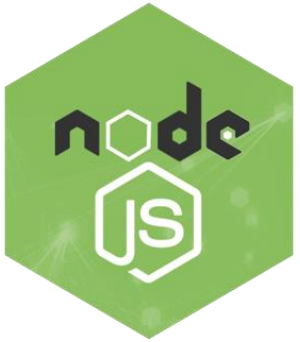
Using traces to map services



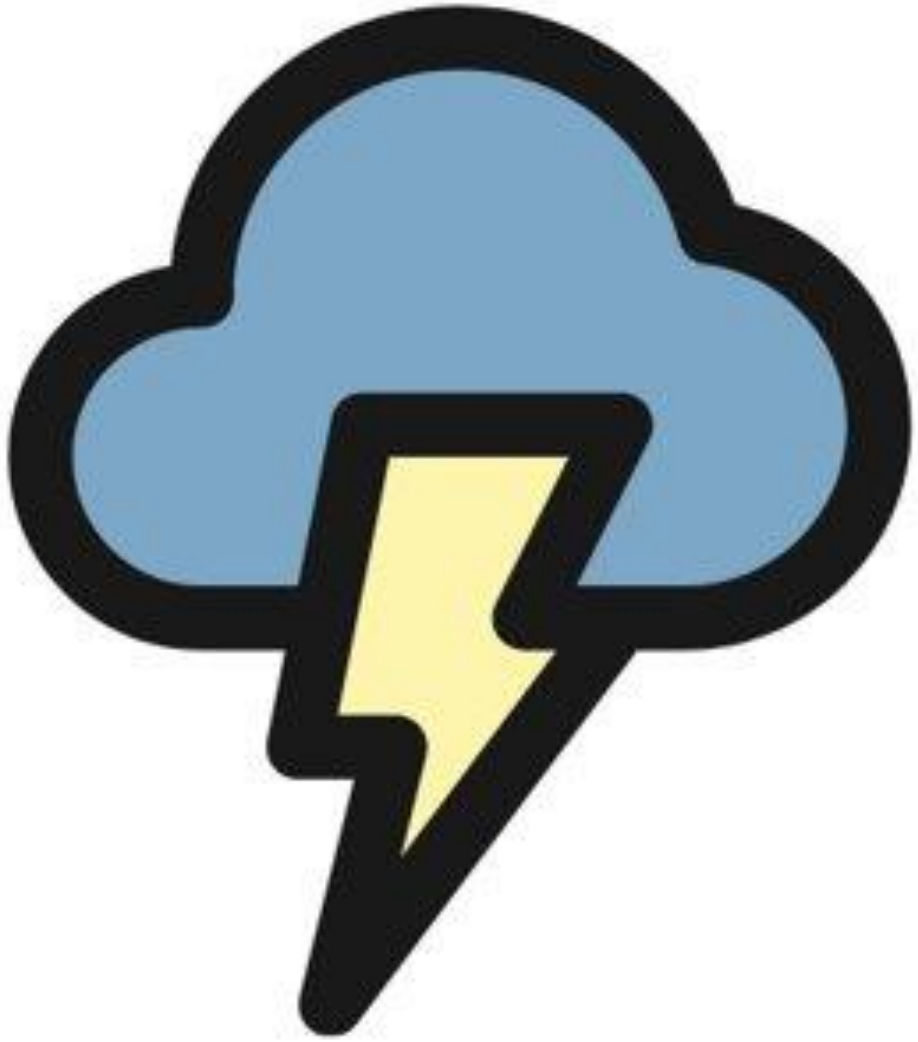
Correlation between signals

OpenTelemetry

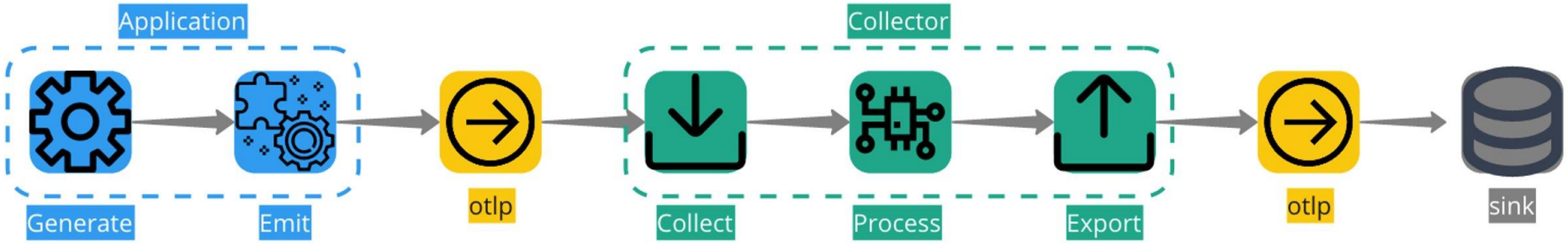
Instrumentation



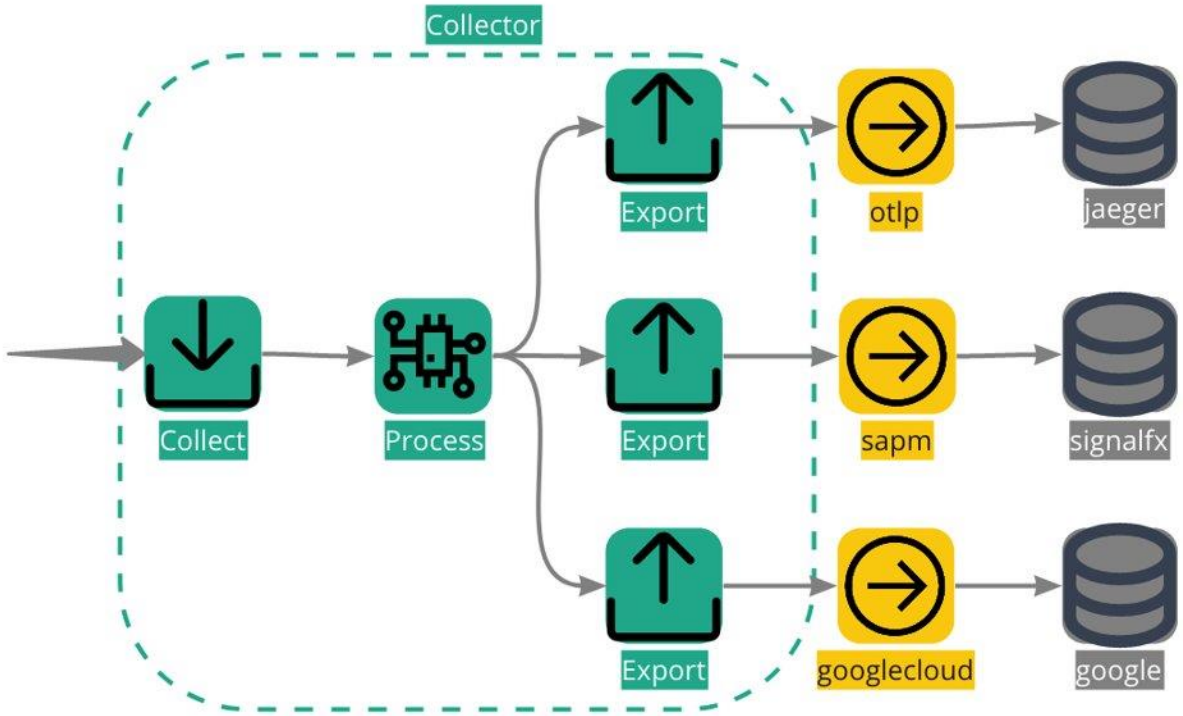
Cloud and Vendor Agnostic



The OpenTelemetry Collector



Collector Contrib and Fan Out



Telemetry Sinks

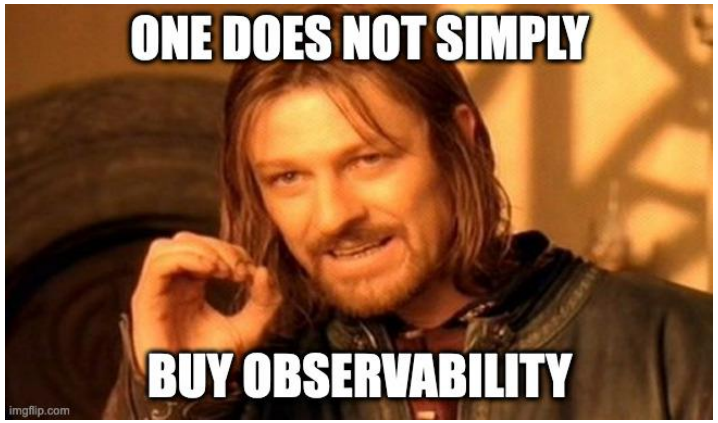
Observability vs Monitoring

I will admit to listening to way too much O11ycast.

Table 9-1. Factors that vary between systems and software

Factor	Your systems	Your software
Rate of change	Package updates (monthly)	Repo commits (daily)
Predictability	High (stable)	Low (many new features)
Value to your business	Low (cost center)	High (revenue generator)
Number of users	Few (internal teams)	Many (your customers)
Core concern	Is the system or service healthy?	Can each request acquire the resources it needs for end-to-end execution in a timely and reliable manner?
Evaluation perspective	The system	Your customers
Evaluation criteria	Low-level kernel and hardware device drivers	Variables and API endpoint
Functional responsibility	Infrastructure operations	Software development
Method for understanding	Monitoring	Observability

https://info.honeycomb.io/observability-engineering-oreilly-book-2022



Observability is not the tooling.

Observability costs money

”It should be a NFR of any project”

Common Challenges in Observability

- Write once, read never database
- Tools as a junk drawer
- Those "I need ALL the data" people
- Dashboards as technical debt
- "You build it, you run it" team decides to run own observability stack
- "What do you mean this isn't a debugging tool?"
- Trying to solve data or business observability issues using only application telemetry.

Site Reliability Engineering

Created by Google

SRE book is freely available

Service Level Agreements
Service Level Objectives
Service Level Indicators

Where do we even begin?

What metrics can we use to describe the critical aspects of our service?

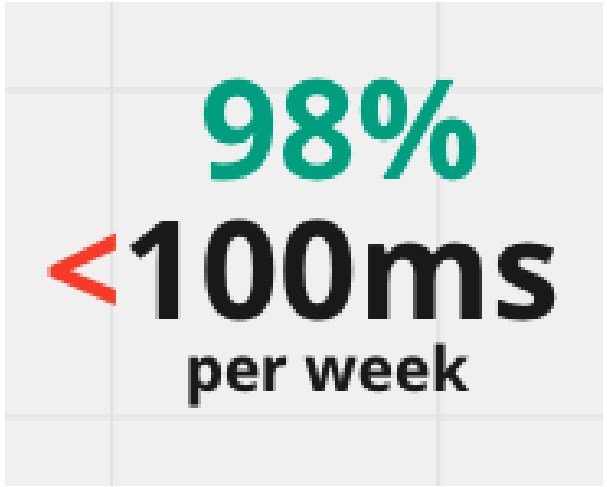
Where is the best place to measure them?

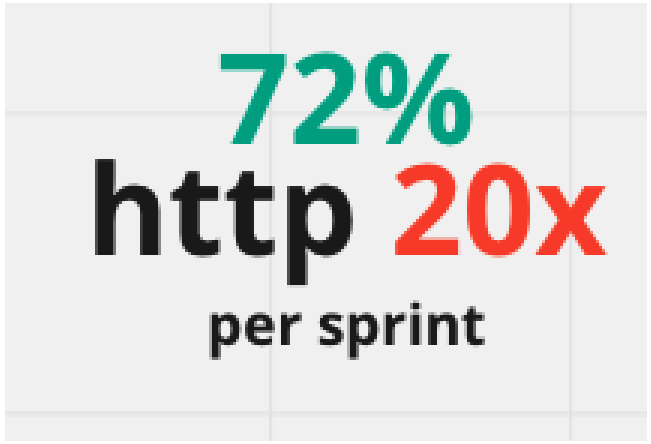
Who is using this service?

What are our Service Level Indicators?

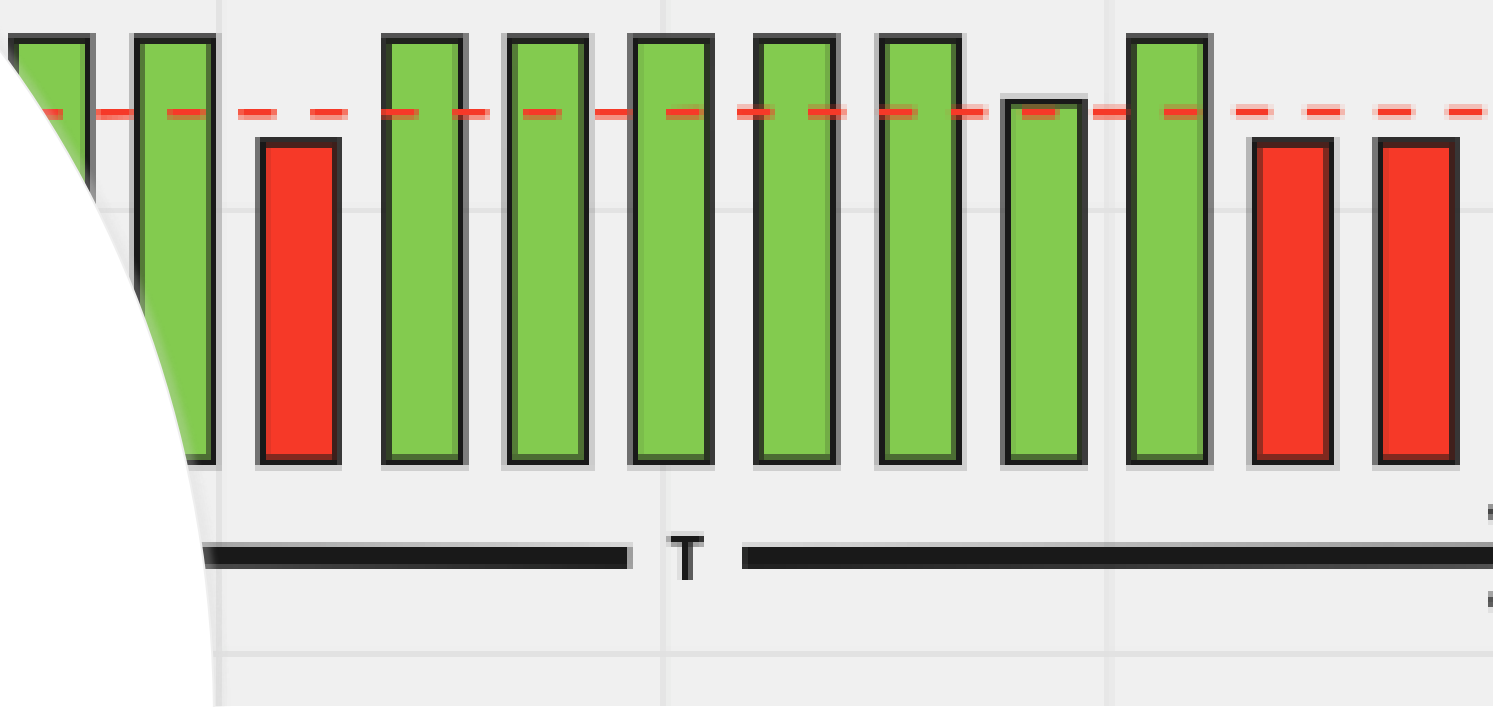
So how is
using metrics for SLOs
different than just
monitoring?

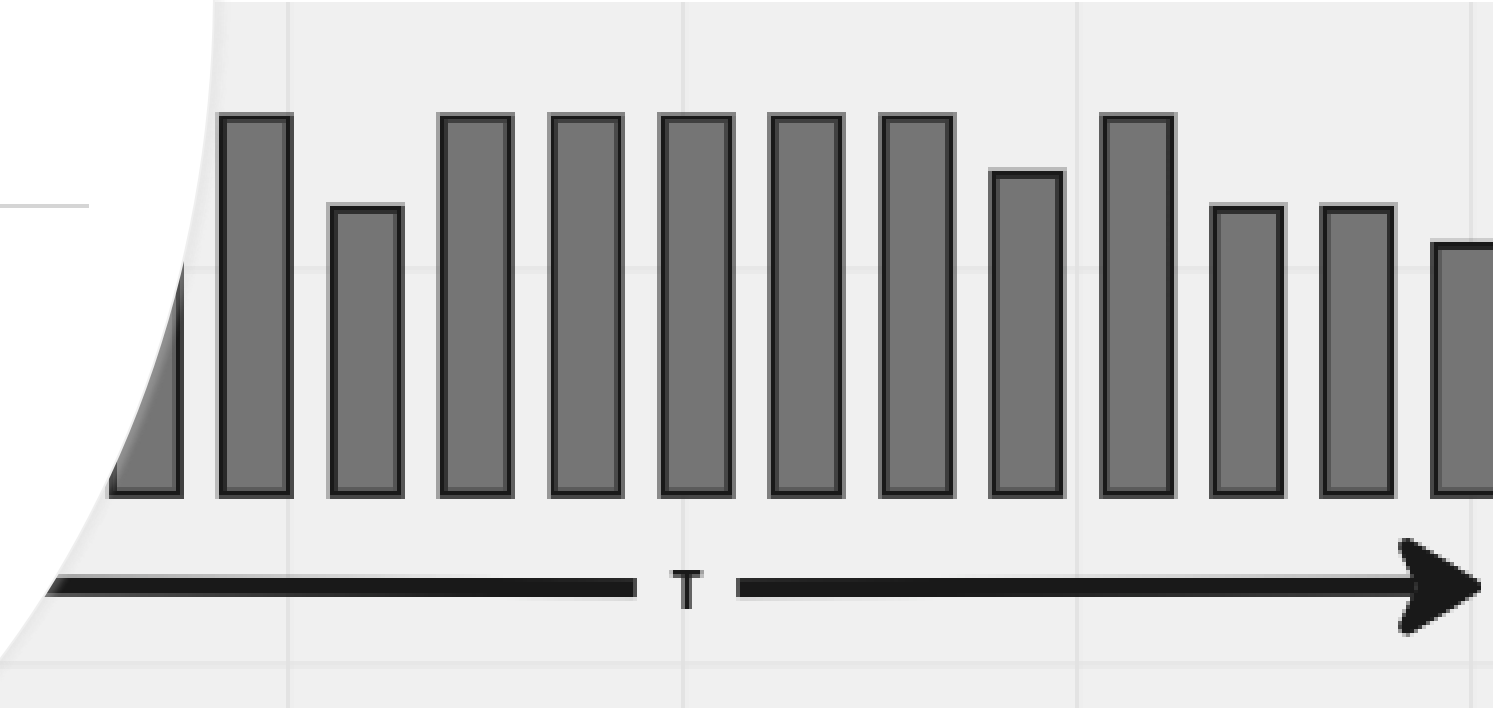
Request based SLIs

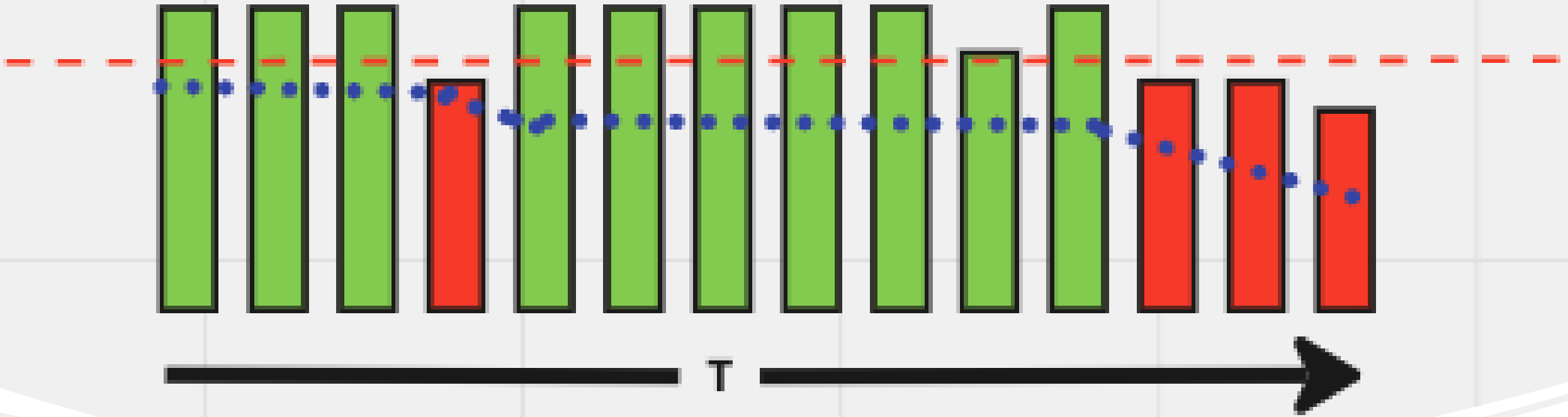




Windows-based SLIs

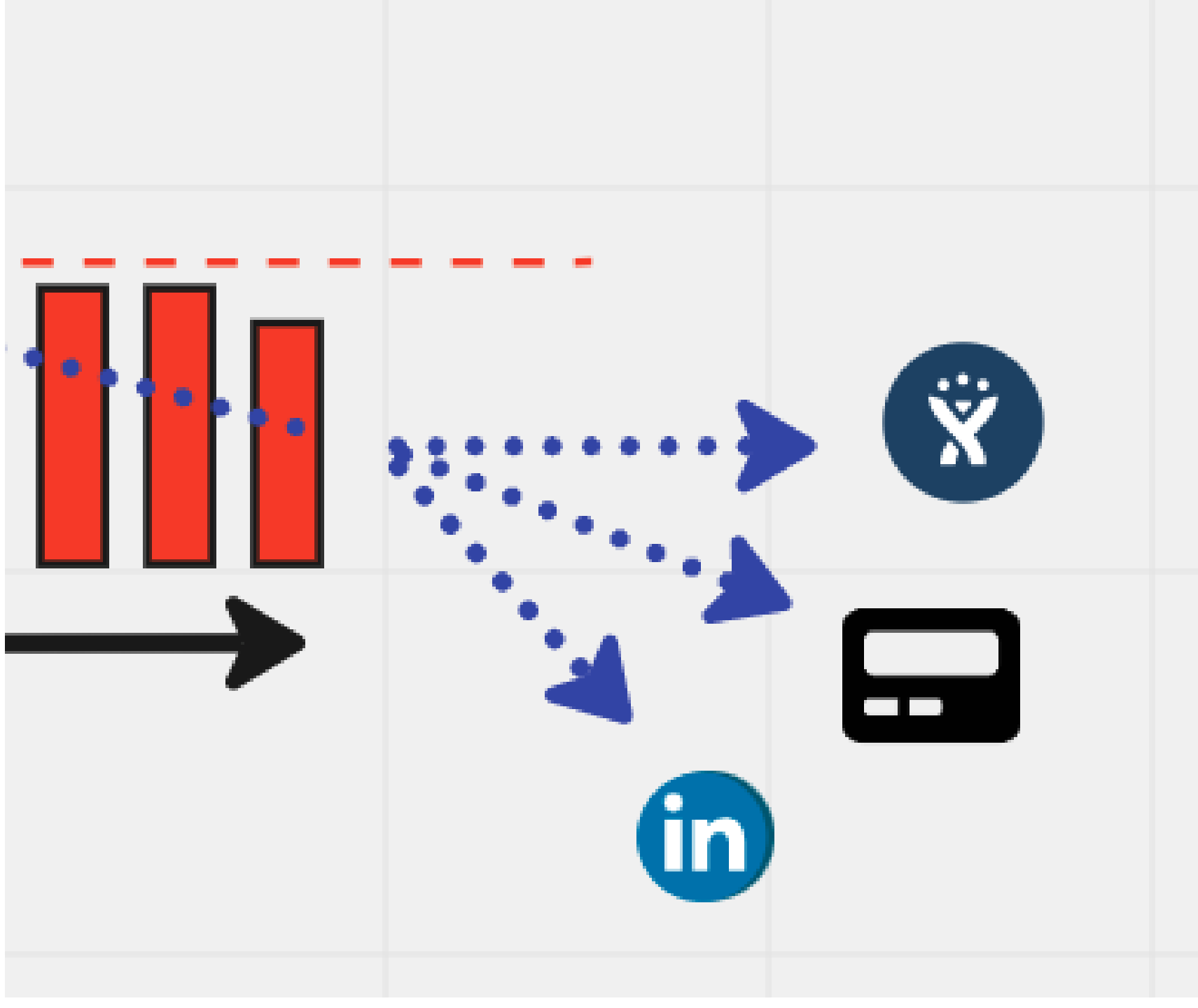






Error Budgets

Burn Rate



It all comes down to time.

Availability and the mythical nine nines

Available minutes / total minutes

Appropriate Reliability

Service Level Agreements

The role of a SLO

Soft limit

Performance expectation

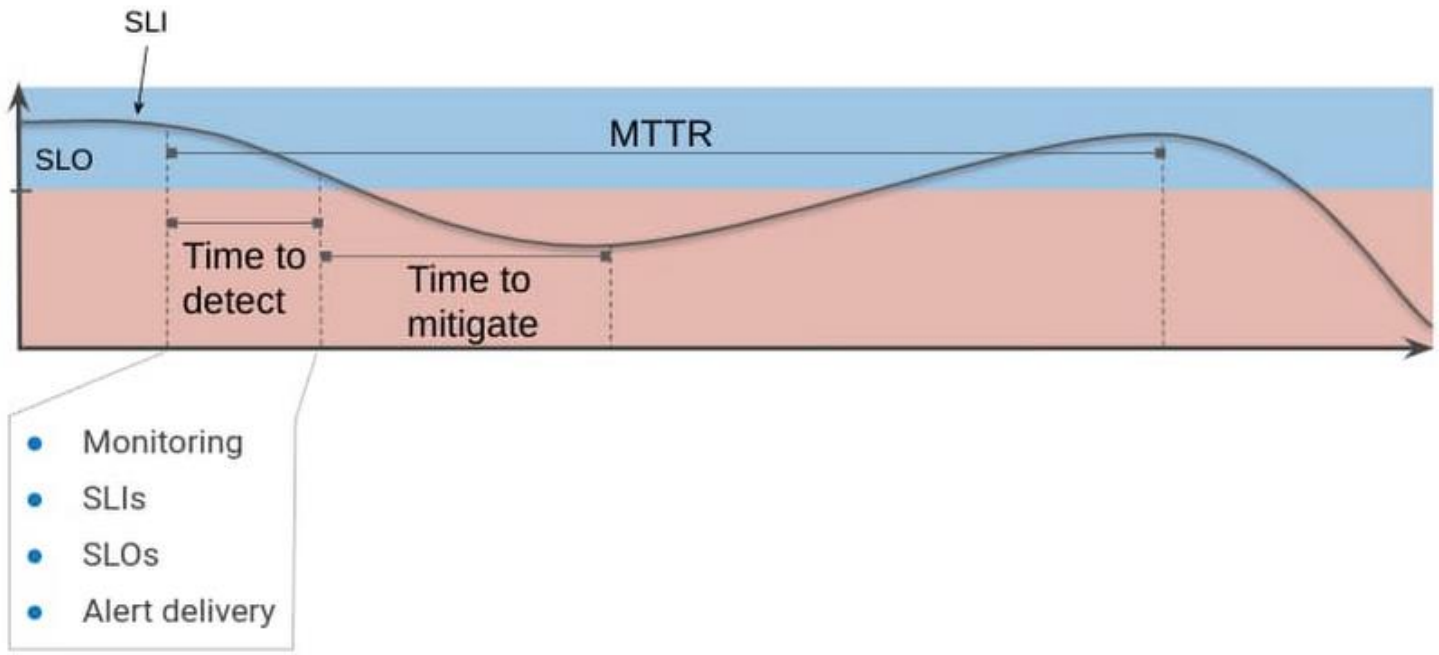
Not a fixed contract

Meant to be revised, reviewed, updated.

Do you engineer for perfection, or do you set reasonable expectations?

SLOs in the wild

But
my service is
feature
driven...



SLOs are your acceptable level of risk

Is it good enough?

Comparing SLOs to ITSI

Philosophical Differences

Free vs Proprietary

Decentralized vs Centralized

Clear boundaries between business and operational data

Tool agnostic vs Splunk specific

Integral component driving discussion between engineers, EM and PO

Design Differences

Measure as close as possible to consumer vs weighted service decomp

SLO data can be collected by APIs*

SLIs vs KPIs

Metrics consumed where they are produced vs single source of truth

DORA metrics vs Event Analytics*

Thoughts?

Are you adopting SRE?

Is anyone mixing SRE and ITSI in production?

Would SLI or SLO data be of any use as a KPI in ITSI?

Is anyone using trace propagation data to create service maps in Splunk?

Thank you

Special thanks to Splunk, Magnus Lord, Thomas Hille and my colleagues in the Observability Pipeline Team

timothy.mahoney1@ingka.ikea.com