THE EVOLUTION OF WEB MONITORING

@EMANUIL_TOLEV

elastic @emanuil_tolev

Community engineer at Elastic.

HISTORY
PRESENT INNOVATION
FUTURE

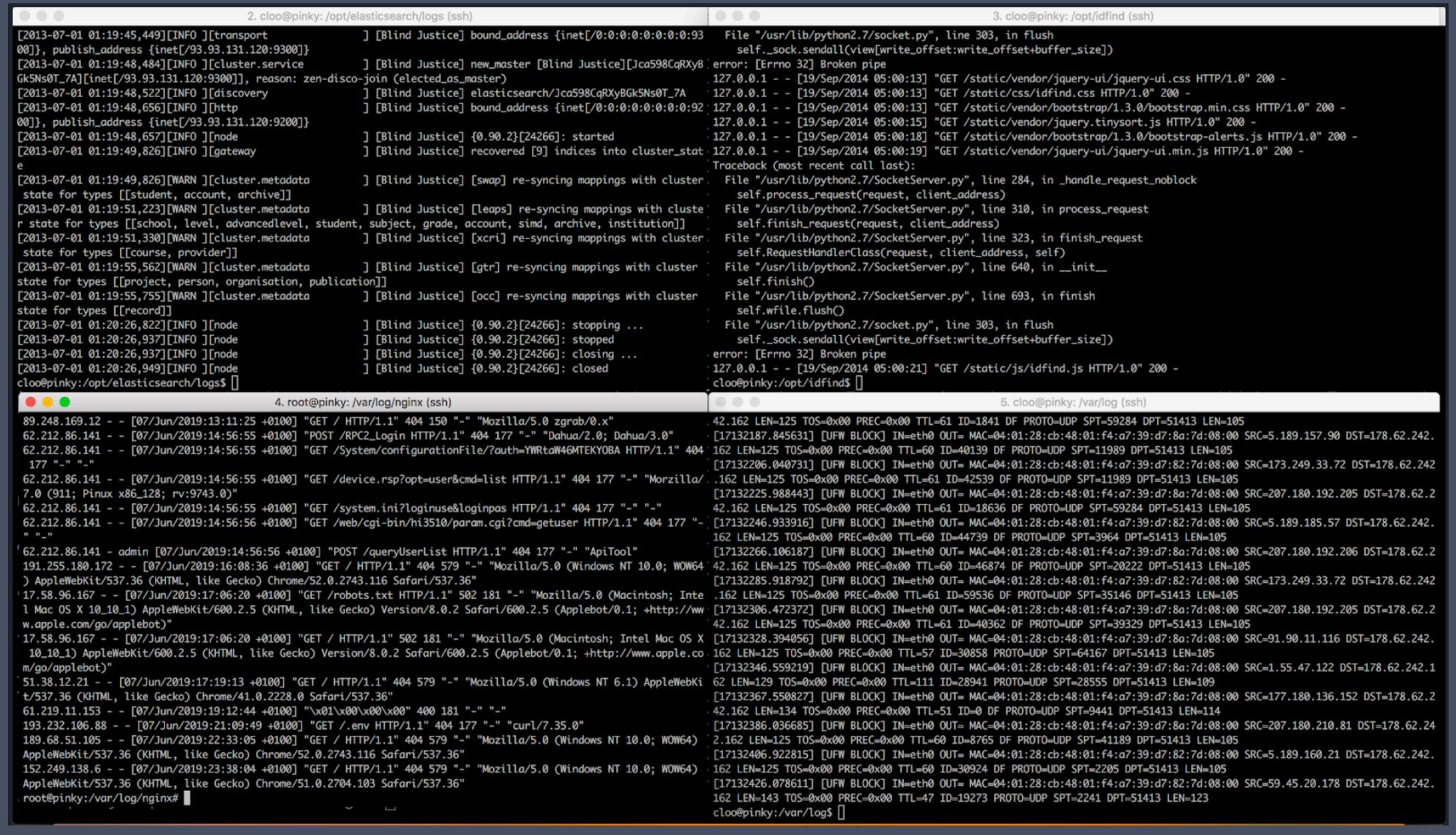
elastic

@emanuil_tolev

```
ess {inet[/93.93.131.120:9200]}
[2013-07-01 00:41:38,099][INFO ][node                     ] [Starsmore, Jonothon] {0.90.2}[23645]: started
[2013-07-01 00:42:18,604][INFO ][node                     ] [Starsmore, Jonothon] {0.90.2}[23645]: stopping ...
[2013-07-01 00:42:18,809][INFO ][node                     ] [Starsmore, Jonothon] {0.90.2}[23645]: stopped
[2013-07-01 00:42:18,809][INFO ][node                     ] [Starsmore, Jonothon] {0.90.2}[23645]: closing ...
[2013-07-01 00:42:19,846][INFO ][node                     ] [Starsmore, Jonothon] {0.90.2}[23645]: closed
[2013-07-01 01:19:43,108][INFO ][node                     ] [Blind Justice] {0.90.2}[24266]: initializing ...
[2013-07-01 01:19:43,114][INFO ][plugins                  ] [Blind Justice] loaded [], sites []
[2013-07-01 01:19:45,340][INFO ][node                     ] [Blind Justice] {0.90.2}[24266]: initialized
[2013-07-01 01:19:45,340][INFO ][node                     ] [Blind Justice] {0.90.2}[24266]: starting ...
[2013-07-01 01:19:45,449][INFO ][transport                ] [Blind Justice] bound_address {inet[/0:0:0:0:0:0:0:0:9300]}, publish_address {i
net[/93.93.131.120:9300]}
[2013-07-01 01:19:48,484][INFO ][cluster.service          ] [Blind Justice] new_master [Blind Justice][Jca598CqRXyBGk5Ns0T_7A][inet[/93.93.
131.120:9300]], reason: zen-disco-join (elected_as_master)
[2013-07-01 01:19:48,522][INFO ][discovery                ] [Blind Justice] elasticsearch/Jca598CqRXyBGk5Ns0T_7A
[2013-07-01 01:19:48,656][INFO ][http                     ] [Blind Justice] bound_address {inet[/0:0:0:0:0:0:0:0:9200]}, publish_address {i
net[/93.93.131.120:9200]}
[2013-07-01 01:19:48,657][INFO ][node                     ] [Blind Justice] {0.90.2}[24266]: started
[2013-07-01 01:19:49,826][INFO ][gateway                  ] [Blind Justice] recovered [9] indices into cluster_state
[2013-07-01 01:19:49,826][WARN ][cluster.metadata         ] [Blind Justice] [swap] re-syncing mappings with cluster state for types [[stude
nt, account, archive]]
[2013-07-01 01:19:51,223][WARN ][cluster.metadata         ] [Blind Justice] [leaps] re-syncing mappings with cluster state for types [[scho
ol, level, advancedlevel, student, subject, grade, account, simd, archive, institution]]
[2013-07-01 01:19:51,330][WARN ][cluster.metadata         ] [Blind Justice] [xcri] re-syncing mappings with cluster state for types [[cours
e, provider]]
[2013-07-01 01:19:55,562][WARN ][cluster.metadata         ] [Blind Justice] [gtr] re-syncing mappings with cluster state for types [[projec
t, person, organisation, publication]]
[2013-07-01 01:19:55,755][WARN ][cluster.metadata         ] [Blind Justice] [occ] re-syncing mappings with cluster state for types [[record
]]
[2013-07-01 01:20:26,822][INFO ][node                     ] [Blind Justice] {0.90.2}[24266]: stopping ...
[2013-07-01 01:20:26,937][INFO ][node                     ] [Blind Justice] {0.90.2}[24266]: stopped
[2013-07-01 01:20:26,937][INFO ][node                     ] [Blind Justice] {0.90.2}[24266]: closing ...
[2013-07-01 01:20:26,949][INFO ][node                     ] [Blind Justice] {0.90.2}[24266]: closed
```

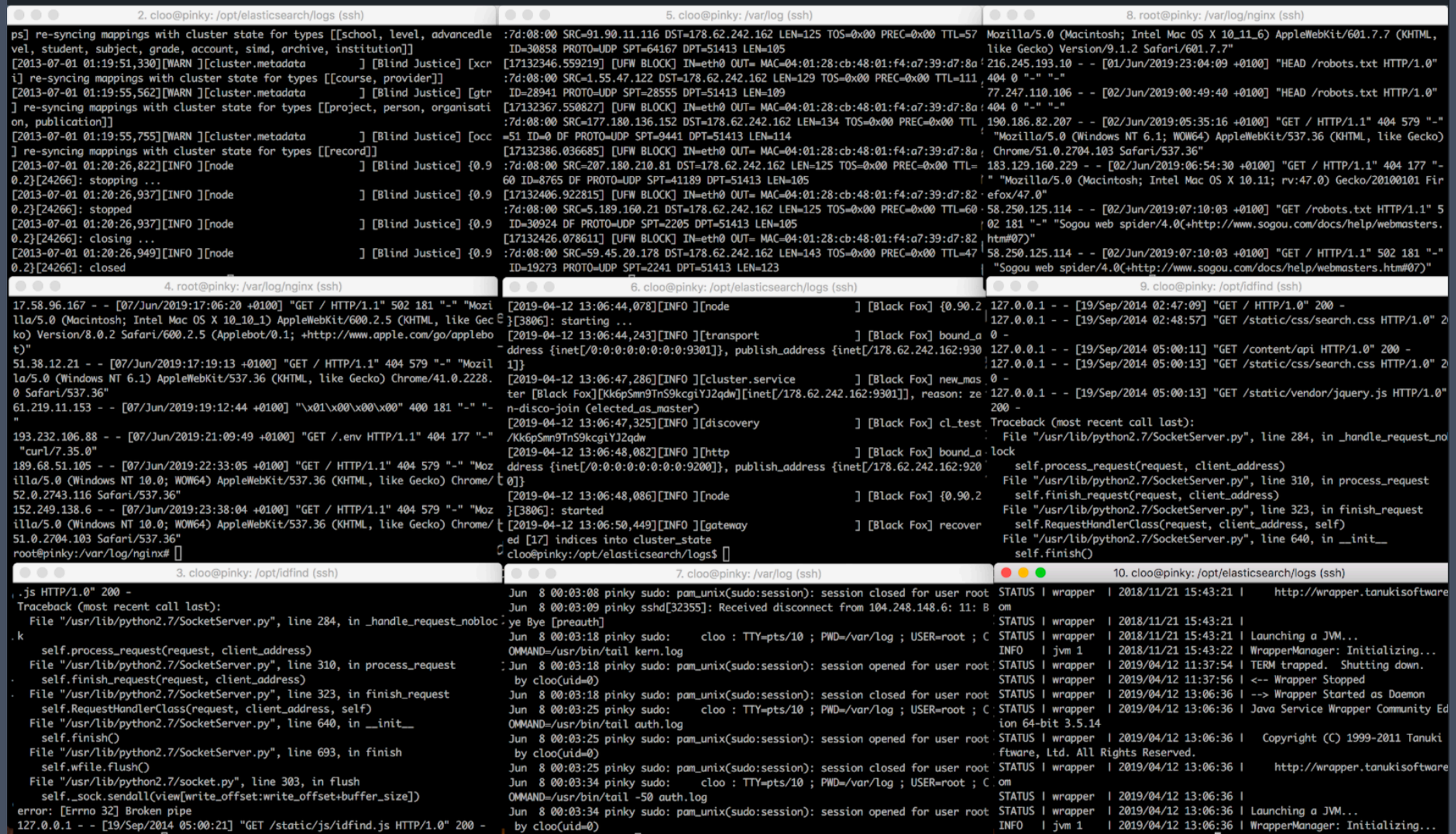
elastic @emanuil_tolev

Logs



elastic @emanuil_tolev

Hmm

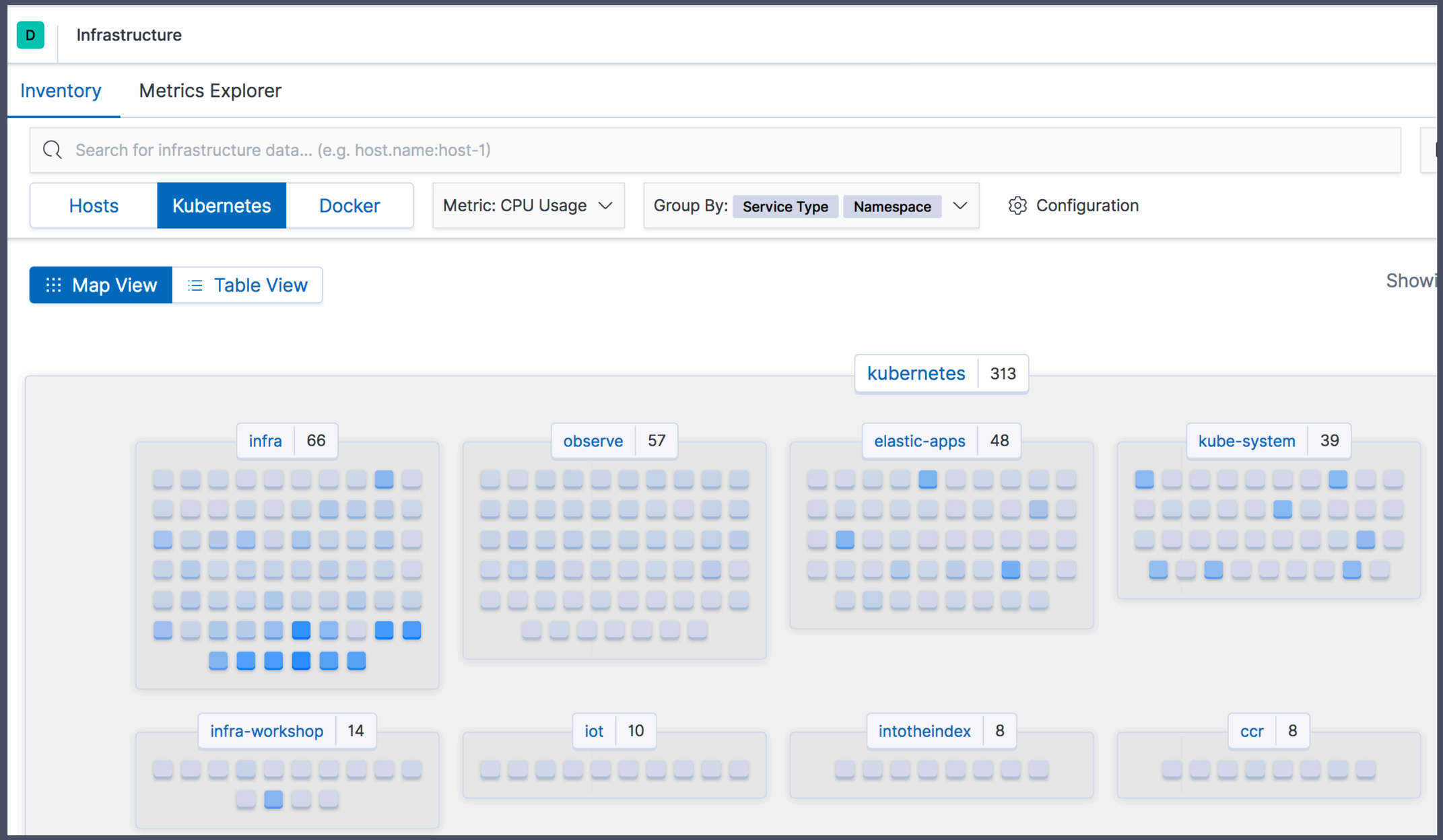


elastic @emanuil_tolev

Well, this is getting challenging to manage

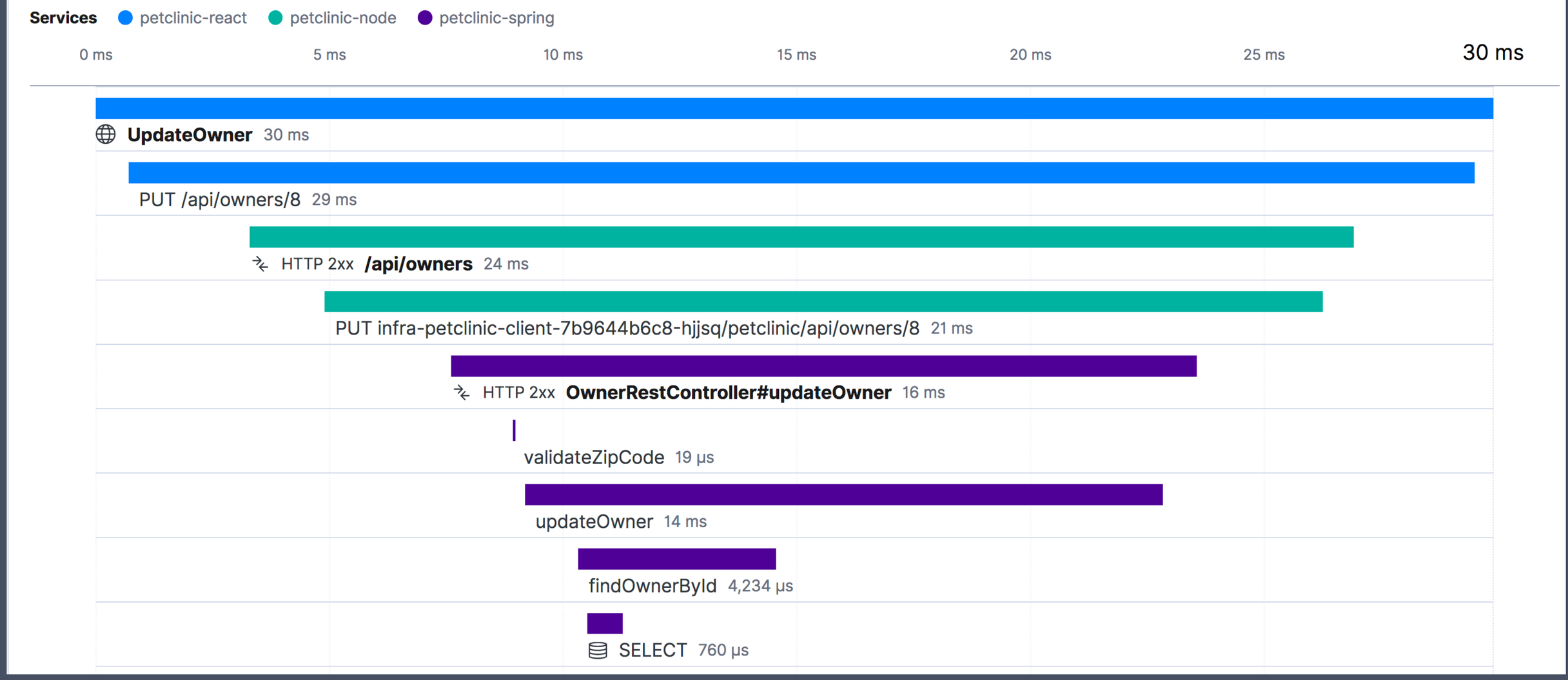
elastic @emanuil_tolev

Very challenging



elastic @emanuil_tolev

metrics



elastic @emanuil_tolev

apm

THE STORY OF MONITORING IS A STORY OF FRUSTRATION, FACEPALMING AND PAINFUL MOMENTS OF REFLECTION

elastic @emanuil_tolev

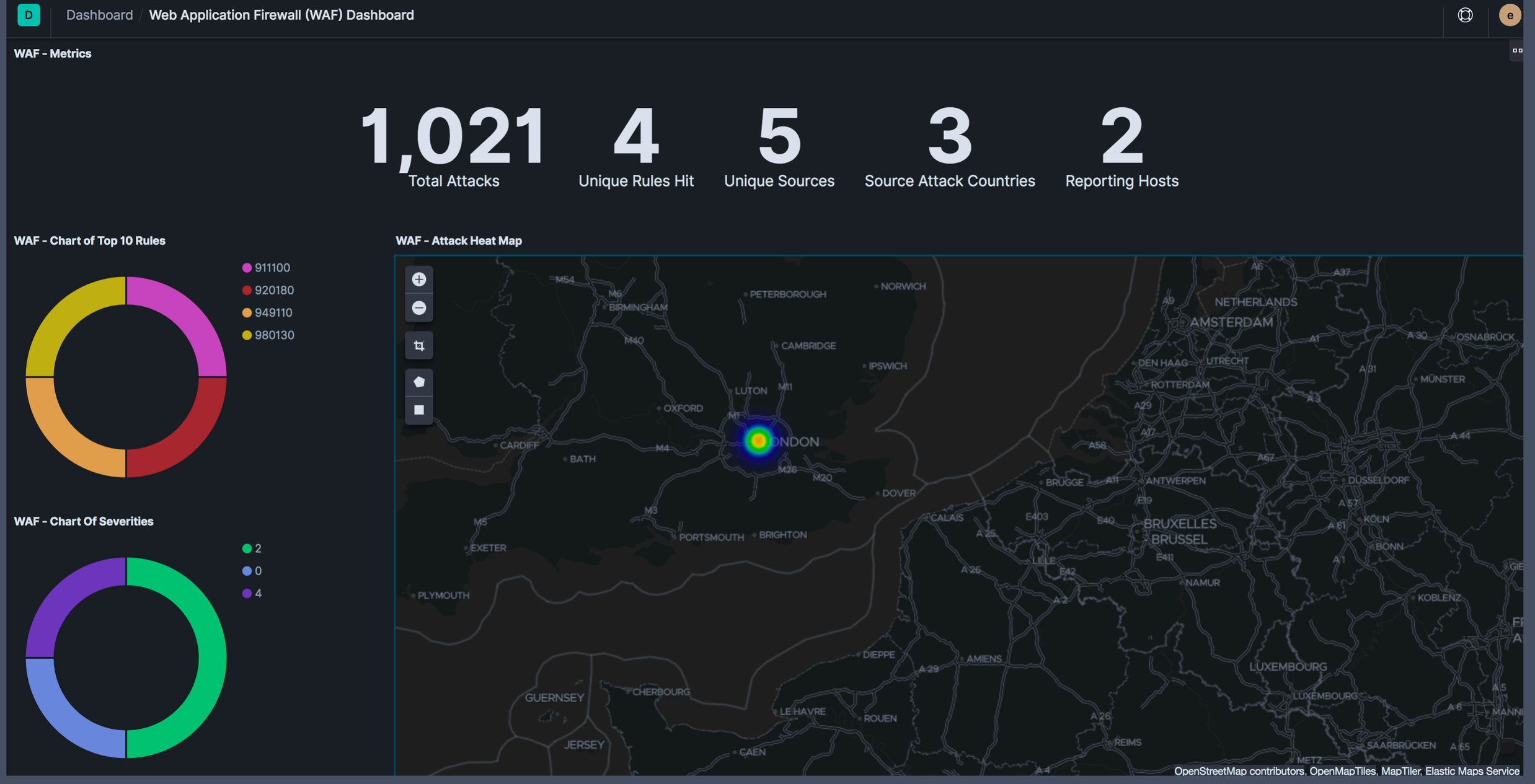
Personal story of managing logs and evolving systems

NOW:

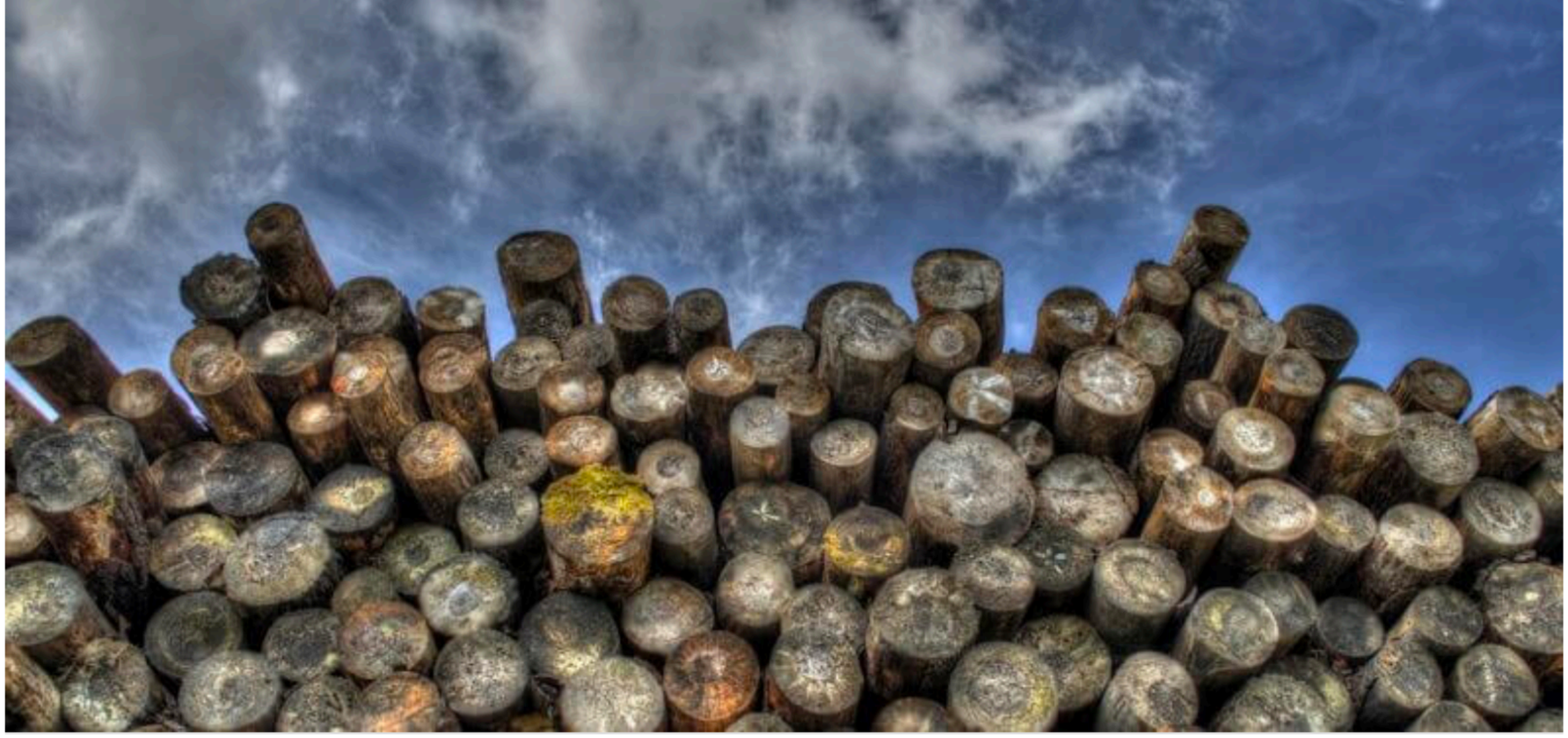
- MONITORING
  - LOGGING
  - METRICS
  - TRACING
- SECURITY?
- OBSERVABILITY

elastic @emanuil_tolev

Elastic is adding security.



we already collect this data anyway, why not use it to secure the systems too. Note you will need special skills though to use a SIEM.



Best Log Management Tools: 51 Useful Tools for Log Management, Monitoring, Analytics, and More

STACKIFY | MAY 26, 2017 | DEVELOPER TIPS, TRICKS & RESOURCES

elastic @emanuil_tolev

Credit to Stackify.com . https://stackify.com/best-log-management-tools/

OBSERVABILITY

HTTPS://WWW.HONEYCOMB.IO/BLOG/OBSERVABILITY-A-MANIFESTO/

elastic @emanuil_tolev

Recommend reading that link if you have not, for a new and different angle. Take a picture now.

Charity Majors from Honeycomb.io [READ VERBATIM!]: "The power to ask new questions of your system, without having to ship new code or gather new data in order to ask those new questions"

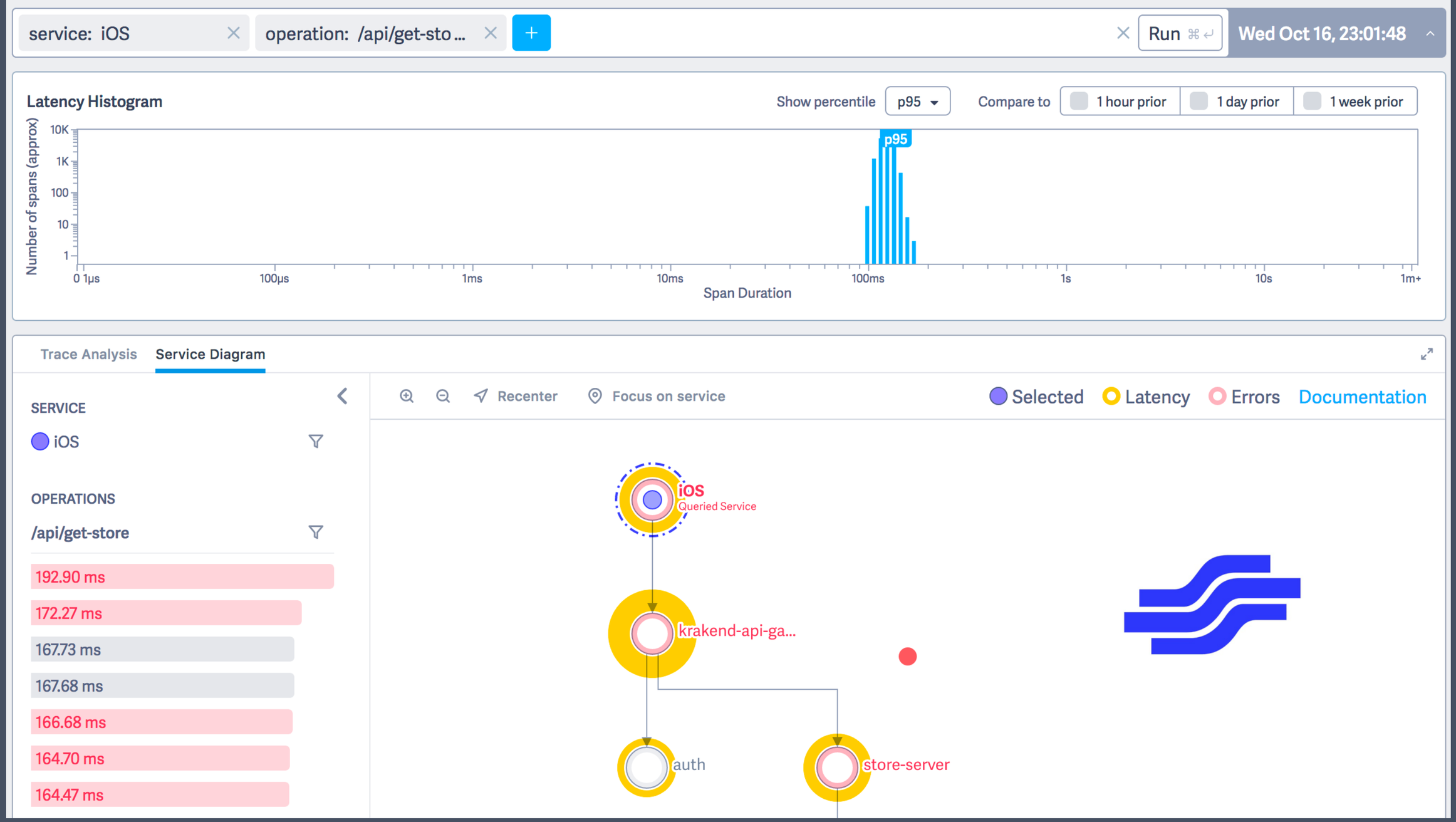
^ "Monitoring is about known-unknowns and actionable alerts, observability is about unknown-unknowns and empowering you to ask arbitrary new questions and explore where the cookie crumbs take you. Observability means you can understand how your systems are working on the inside just by asking questions from outside."

PRESENT INNOVATION

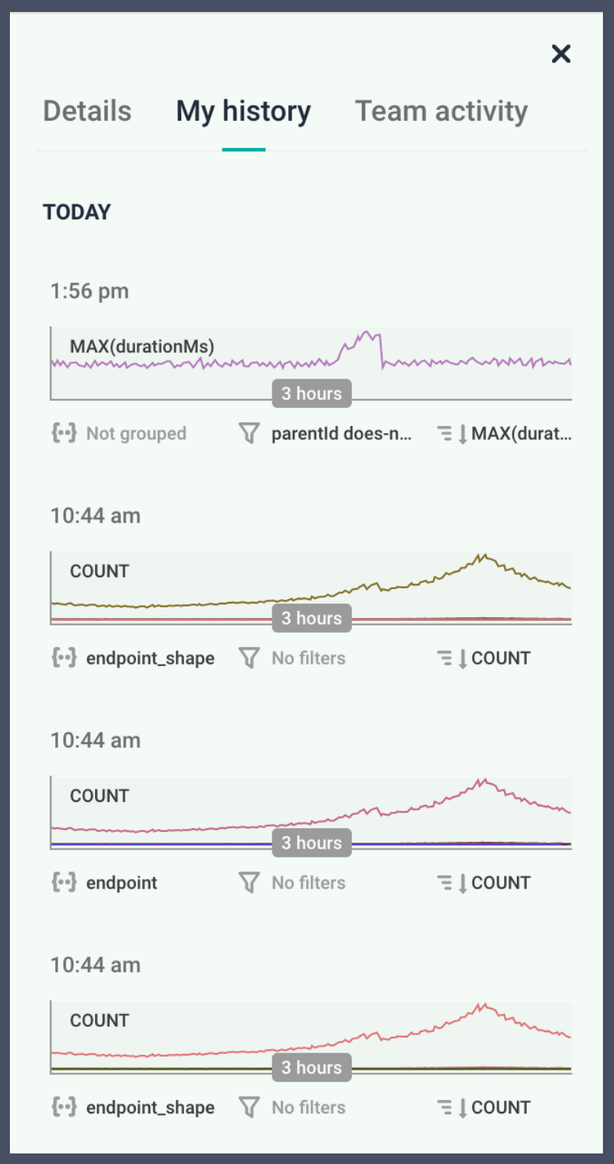
- FEATURES
- BUSINESS MODELS
- STRATEGIC VIEW OF OPS PAIN & RELIEF

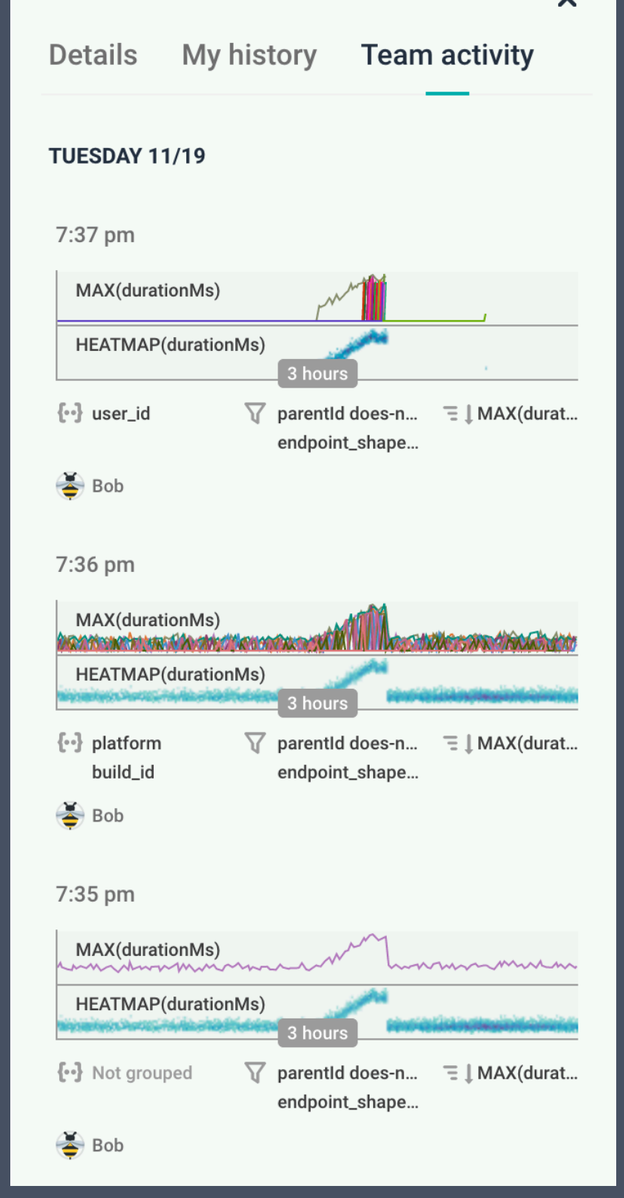
elastic

@emanuil_tolev



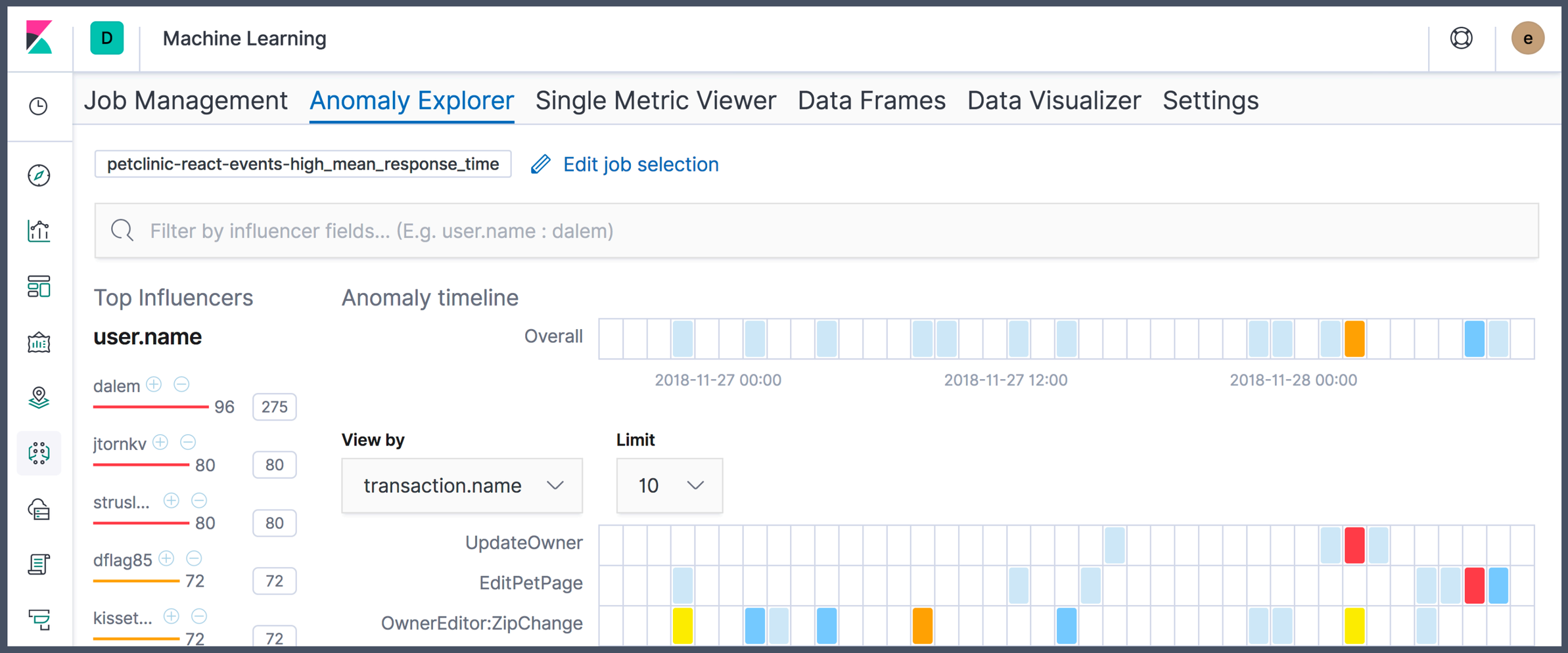
Kind of hard to explain but basically it's a service diagram like you would see in Newrelic and Datadog etc. but. This one overlays the deepest layer (furthest back) at which a specific error is detected. This screenshot shows trying to diagnose a specific problem, it's from their public demo.





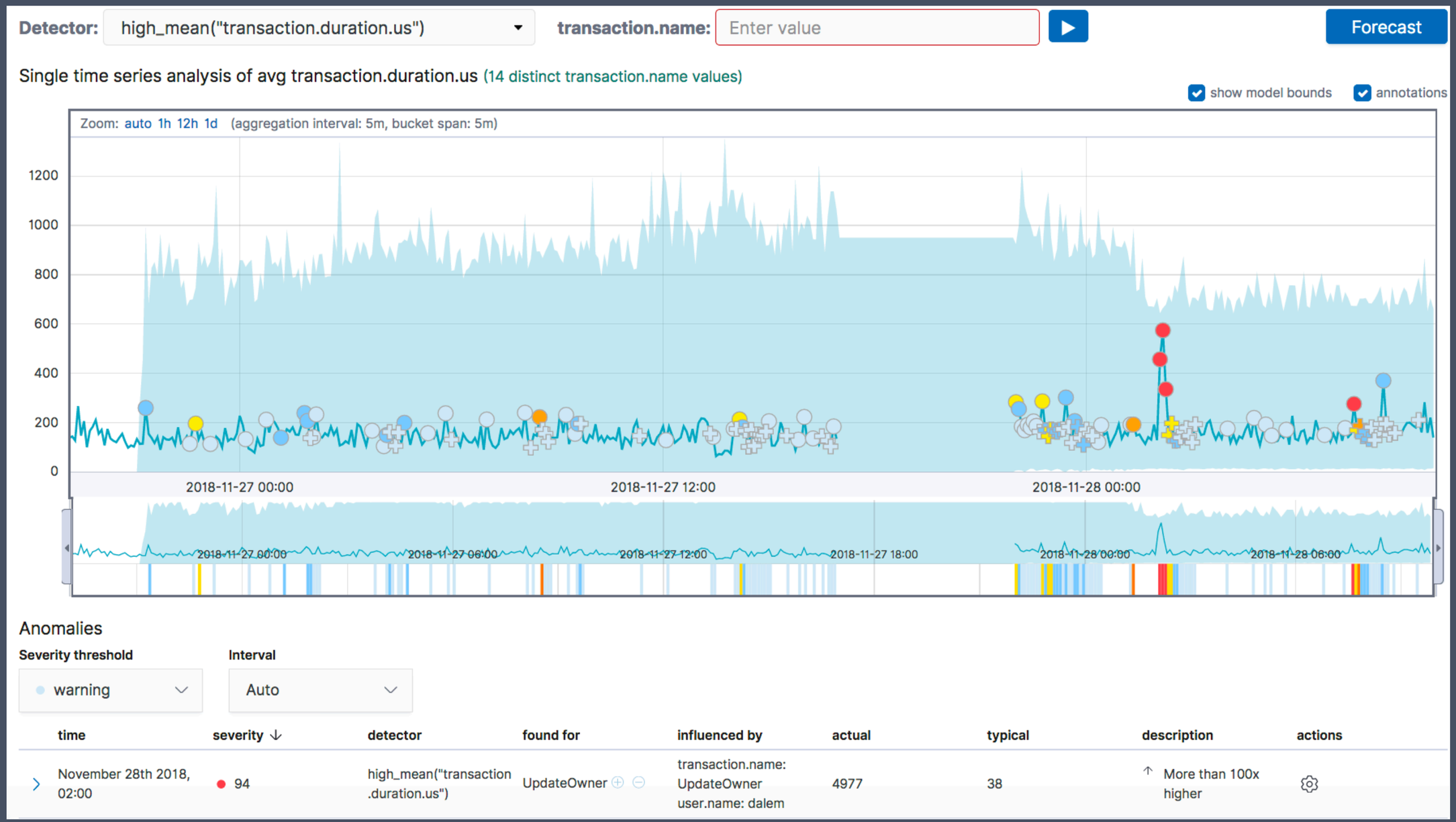
elastic @emanuil_tolev

Shows what you yourself looked at – useful at retro. Shows what other ppl looked at - collaborative. Encapsulates team knowledge. An advanced version could be used for training juniors? Writing disaster recovery playbooks straight in your troubleshooting tool?



elastic @emanuil_tolev

Paid but we are talking about innovation of any kind. This is very cool. Anomaly detection. Unlabeled, I didn't tell it to look at user.name and transaction.name - it thinks there is correlation between slowdown and these features in the dataset.



elastic @emanuil_tolev

a view of the model

BUSINESS MODELS

VARIETY: CHARGE PER NODE / DATA VOLUME / DATA STORAGE / COMPUTE / OPS USER. ...

elastic @emanuil_tolev

Vary. Elastic tends to aim for resources used rather than per collector agent running.

STRATEGIC VIEW

- HONEYCOMB: EVENTS, STRUCTURED INFO RATHER THAN LOGS, UNKNOWN UNKNOWNS, THE SYSTEM TEACHES US
- ELASTIC AND SPLUNK: ONE-STOP SHOP (BUT PRICING VARIES BY ORDERS OF MAGNITUDE IN DIFF USE CASES)
- MANY OTHERS

elastic @emanuil_tolev

The very framing itself changes how the companies look at things. Honeycomb, Lightspeed and Elastic APM likely cannot be compared head to head because the philosophical (or framing) differences run too deep.

THE FUTURE

- IN-DEPTH COMPARISON OF VENDORS?
- TRYING EVERY TOOL AVAILABLE AND WRITING A BOOK?
- PRODUCT MANAGERS @ VENDORS DECIDE WHERE NEXT?
- TIME-TESTED METHOD: GO RANT AT SEVERAL CONFERENCES ABOUT YOUR OWN FRUSTRATIONS!

nobody got time for that first one. Nobody practicing ops actively, plus I can't do it while working for a vendor. No time for 2nd item either I reckon.

^ if you have opinions, some vendors do listen and hear them, easiest way to influence.

^ of course, remember to rant at us^H^H give feedback ;). etolev@elastic.co