

THE EVOLUTION OF WEB MONITORING



@EMANUIL_TOLEV



@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[/0:0:0:0:0:0:0:9300]}, publish_address {inet[/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[/0:0:0:0:0:0:0:9200]}, publish_address {inet[/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 [[student, account, archive]]
[2013-07-01 01:19:51,223][WARN ][cluster.metadata] [Blind Justice] [leaps] re-syncing mappings with cluster state for types [[school, 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 [[course, provider]]
[2013-07-01 01:19:55,562][WARN ][cluster.metadata] [Blind Justice] [gtr] re-syncing mappings with cluster state for types [[project, 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
```



@emanuil_tolev

Logs

```

2. cloo@pinky: /opt/elasticsearch/logs (ssh)
[2013-07-01 01:19:45,449][INFO ][transport] [Blind Justice] bound_address {inet[/0:0:0:0:0:0:0:9300]}, publish_address {inet[/93.93.131.120:9300]}
[2013-07-01 01:19:48,484][INFO ][cluster.service] [Blind Justice] new_master [Blind Justice][Jca598CqRXyB] reason: zen-disco-join (elected_as_master)
[GNSs0T_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[/0:0:0:0:0:0:0:9200]}, publish_address {inet[/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_stat
e
[2013-07-01 01:19:49,826][WARN ][cluster.metadata] [Blind Justice] [swap] re-syncing mappings with cluster state for types [[student, account, archive]]
[2013-07-01 01:19:51,223][WARN ][cluster.metadata] [Blind Justice] [leaps] re-syncing mappings with cluster state for types [[school, 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 [[course, provider]]
[2013-07-01 01:19:55,562][WARN ][cluster.metadata] [Blind Justice] [gtr] re-syncing mappings with cluster state for types [[project, 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
cloo@pinky:/opt/elasticsearch/logs$ 
```

```

3. cloo@pinky: /opt/dfind (ssh)
File "/usr/lib/python2.7/socket.py", line 303, in flush
    self._sock.sendall(view[write_offset:write_offset+buffer_size])
error: [Errno 32] Broken pipe
127.0.0.1 - - [19/Sep/2014 05:00:13] "GET /static/vendor/jquery-ui/jquery-ui.css HTTP/1.0" 200 -
127.0.0.1 - - [19/Sep/2014 05:00:13] "GET /static/css/dfind.css HTTP/1.0" 200 -
127.0.0.1 - - [19/Sep/2014 05:00:13] "GET /static/vendor/bootstrap/1.3.0/bootstrap.min.css HTTP/1.0" 200 -
127.0.0.1 - - [19/Sep/2014 05:00:15] "GET /static/vendor/tinysort.js HTTP/1.0" 200 -
127.0.0.1 - - [19/Sep/2014 05:00:18] "GET /static/vendor/bootstrap/1.3.0/bootstrap-alerts.js HTTP/1.0" 200 -
127.0.0.1 - - [19/Sep/2014 05:00:19] "GET /static/vendor/jquery-ui/jquery-ui.min.js HTTP/1.0" 200 -
Traceback (most recent call last):
  File "/usr/lib/python2.7/SocketServer.py", line 284, in _handle_request_noblock
    self._process_request(request, client_address)
  File "/usr/lib/python2.7/SocketServer.py", line 310, in _process_request
    self._finish_request(request, client_address)
  File "/usr/lib/python2.7/SocketServer.py", line 323, in _finish_request
    self._RequestHandlerClass(request, client_address, self)
  File "/usr/lib/python2.7/SocketServer.py", line 640, in __init__
    self._finish()
  File "/usr/lib/python2.7/SocketServer.py", line 693, in finish
    self.wfile.flush()
  File "/usr/lib/python2.7/socket.py", line 303, in flush
    self._sock.sendall(view[write_offset:write_offset+buffer_size])
error: [Errno 32] Broken pipe
127.0.0.1 - - [19/Sep/2014 05:00:21] "GET /static/js/dfind.js HTTP/1.0" 200 -
cloo@pinky:/opt/dfind$ 
```

```

4. root@pinky: /var/log/nginx (ssh)
89.248.169.12 - - [07/Jun/2019:13:11:25 +0100] "GET / HTTP/1.1" 404 150 "-" "Mozilla/5.0 zgrab/0.x"
62.212.86.141 - - [07/Jun/2019:14:56:55 +0100] "POST /RPC2_Login HTTP/1.1" 404 177 "-" "Dahua/2.0; Dahua/3.0"
62.212.86.141 - - [07/Jun/2019:14:56:55 +0100] "GET /System/configurationFile/?auth=YWRtaW46MTEKY0BA HTTP/1.1" 404 177 "-" "-"
62.212.86.141 - - [07/Jun/2019:14:56:55 +0100] "GET /device.rsp?opt=user&cmd=list HTTP/1.1" 404 177 "-" "Morzilla/7.0 (911; Linux x86_128; rv:9743.0)"
62.212.86.141 - - [07/Jun/2019:14:56:55 +0100] "GET /system.ini?login&loginpas HTTP/1.1" 404 177 "-" "-"
62.212.86.141 - - [07/Jun/2019:14:56:56 +0100] "GET /web/cgi-bin/his3510/param.cgi?cmd=getuser HTTP/1.1" 404 177 "-"-
62.212.86.141 - admin [07/Jun/2019:14:56:56 +0100] "POST /queryUserList HTTP/1.1" 404 177 "-" "ApiTool"
191.255.180.172 - - [07/Jun/2019:16:08:36 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WO
NG4 ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
17.58.96.167 - - [07/Jun/2019:17:06:20 +0100] "GET /robots.txt HTTP/1.1" 502 181 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10.1) AppleWebKit/600.2.5 (KHTML, like Gecko) Version/8.0.2 Safari/600.2.5 (Applebot/0.1; +http://www.apple.com/go/applebot)"
17.58.96.167 - - [07/Jun/2019:17:06:20 +0100] "GET / HTTP/1.1" 502 181 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10.1) AppleWebKit/600.2.5 (KHTML, like Gecko) Version/8.0.2 Safari/600.2.5 (Applebot/0.1; +http://www.apple.co
m/go/applebot)"
51.38.12.21 - - [07/Jun/2019:17:19:13 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36"
61.219.11.153 - - [07/Jun/2019:19:12:44 +0100] "\x01\x00\x00\x00" 400 181 "-"-
193.232.106.88 - - [07/Jun/2019:21:09:49 +0100] "GET /.env HTTP/1.1" 404 177 "-" "curl/7.35.0"
189.68.51.105 - - [07/Jun/2019:22:33:05 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WO
NG4 ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
152.249.138.6 - - [07/Jun/2019:23:38:04 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WO
NG4 ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"
root@pinky:/var/log/nginx# 
```



@emanuil_tolev

Hmm

Host	Log Type	Content
2. cloo@pinky: /opt/elasticsearch/logs (ssh)	System Log	ps] re-syncing mappings with cluster state for types [[school, level, advancedlevel, student, subject, grade, account, simd, archive, institution]] [2013-07-01 01:19:51,330][WARN][cluster.metadata] [Blind Justice] [xcr] i] re-syncing mappings with cluster state for types [[course, provider]] [2013-07-01 01:19:55,562][WARN][cluster.metadata] [Blind Justice] [gtr]] re-syncing mappings with cluster state for types [[project, person, organization, 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] {0.9} 0.2][24266]: stopping ... [2013-07-01 01:20:26,937][INFO][node] [Blind Justice] {0.9} 0.2][24266]: stopped [2013-07-01 01:20:26,937][INFO][node] [Blind Justice] {0.9} 0.2][24266]: closing ... [2013-07-01 01:20:26,949][INFO][node] [Blind Justice] {0.9} 0.2][24266]: closed
5. cloo@pinky: /var/log (ssh)	System Log	:7d:08:00 SRC=91.90.11.116 DST=178.62.242.162 LEN=125 TOS=0x00 PREC=0x00 TTL=57 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7" ID=30858 PROTO=UDP SPT=64167 DPT=51413 LEN=105 [17132346.559219] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a :7d:08:00 SRC=1.55.47.122 DST=178.62.242.162 LEN=129 TOS=0x00 PREC=0x00 TTL=111 77.247.110.106 -- [02/Jun/2019:00:49:40 +0100] "HEAD /robots.txt HTTP/1.0" ID=28941 PROTO=UDP SPT=28555 DPT=51413 LEN=109 [17132367.550827] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a :7d:08:00 SRC=177.180.136.152 DST=178.62.242.162 LEN=134 TOS=0x00 PREC=0x00 TTL=51 ID=0 DF PROTO=UDP SPT=9441 DPT=51413 LEN=114 [17132386.036685] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:8a :7d:08:00 SRC=207.180.210.81 DST=178.62.242.162 LEN=125 TOS=0x00 PREC=0x00 TTL=60 ID=8765 DF PROTO=UDP SPT=41189 DPT=51413 LEN=105 [17132406.922815] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82 :7d:08:00 SRC=5.189.160.21 DST=178.62.242.162 LEN=125 TOS=0x00 PREC=0x00 TTL=60 ID=30924 DF PROTO=UDP SPT=2205 DPT=51413 LEN=105 [17132426.078611] [UFW BLOCK] IN=eth0 OUT= MAC=04:01:28:cb:48:01:f4:a7:39:d7:82 :7d:08:00 SRC=59.45.20.178 DST=178.62.242.162 LEN=143 TOS=0x00 PREC=0x00 TTL=47 ID=19273 PROTO=UDP SPT=2241 DPT=51413 LEN=123
8. root@pinky: /var/log/nginx (ssh)	System Log	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7" 216.245.193.10 -- [01/Jun/2019:23:04:09 +0100] "HEAD /robots.txt HTTP/1.0" 77.247.110.106 -- [02/Jun/2019:00:49:40 +0100] "HEAD /robots.txt HTTP/1.0" 190.186.82.207 -- [02/Jun/2019:05:35:16 +0100] "GET / HTTP/1.1" 404 579 "-" Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" 183.129.160.229 -- [02/Jun/2019:06:54:30 +0100] "GET / HTTP/1.1" 404 177 "-" Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11; rv:47.0) Gecko/20100101 Firefox/47.0" 58.250.125.114 -- [02/Jun/2019:07:10:03 +0100] "GET /robots.txt HTTP/1.1" 502 181 "-" Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)" 58.250.125.114 -- [02/Jun/2019:07:10:03 +0100] "GET / HTTP/1.1" 502 181 "-" Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
4. root@pinky: /var/log/nginx (ssh)	System Log	17.58.96.167 -- [07/Jun/2019:17:06:20 +0100] "GET / HTTP/1.1" 502 181 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/600.2.5 (KHTML, like Gecko) Version/8.0.2 Safari/600.2.5 (Applebot/0.1; +http://www.apple.com/go/applebot)" 51.38.12.21 -- [07/Jun/2019:17:19:13 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36" 61.219.11.153 -- [07/Jun/2019:19:12:44 +0100] "\x01\x00\x00\x00" 400 181 "-" "193.232.106.88 -- [07/Jun/2019:21:09:49 +0100] "GET /.env HTTP/1.1" 404 177 "-" "curl/7.35.0" 189.68.51.105 -- [07/Jun/2019:22:33:05 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36" 152.249.138.6 -- [07/Jun/2019:23:38:04 +0100] "GET / HTTP/1.1" 404 579 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" root@pinky:/var/log/nginx# []
6. cloo@pinky: /opt/elasticsearch/logs (ssh)	System Log	[2019-04-12 13:06:44,078][INFO][node] [Black Fox] {0.90.2} [3806]: starting ... [2019-04-12 13:06:44,243][INFO][transport] [Black Fox] bound_address {inet[/0:0:0:0:0:0:0:9301]}, publish_address {inet[/178.62.242.162:9301]} [2019-04-12 13:06:47,286][INFO][cluster.service] [Black Fox] new_master [Kk6pSmn9TnS9kcgijYJ2qdw][inet[/178.62.242.162:9301]], reason: zen-disco-join (elected_as_master) [2019-04-12 13:06:47,325][INFO][discovery] [Black Fox] cl_test /Kk6pSmn9TnS9kcgijYJ2qdw [2019-04-12 13:06:48,082][INFO][http] [Black Fox] bound_address {inet[/0:0:0:0:0:0:9200]}, publish_address {inet[/178.62.242.162:9200]} [2019-04-12 13:06:48,086][INFO][node] [Black Fox] {0.90.2} [3806]: started [2019-04-12 13:06:50,449][INFO][gateway] [Black Fox] recover ed [17] indices into cluster_state cloo@pinky:/opt/elasticsearch/logs\$ []
9. cloo@pinky: /opt/idfind (ssh)	System Log	127.0.0.1 -- [19/Sep/2014 02:47:09] "GET / HTTP/1.0" 200 - 127.0.0.1 -- [19/Sep/2014 02:48:57] "GET /static/css/search.css HTTP/1.0" 200 - 127.0.0.1 -- [19/Sep/2014 05:00:11] "GET /content/api HTTP/1.0" 200 - 127.0.0.1 -- [19/Sep/2014 05:00:13] "GET /static/css/search.css HTTP/1.0" 200 - 127.0.0.1 -- [19/Sep/2014 05:00:13] "GET /static/vendor/jquery.js HTTP/1.0" 200 - Traceback (most recent call last): File "/usr/lib/python2.7/SocketServer.py", line 284, in _handle_request_no lock self.process_request(request, client_address) File "/usr/lib/python2.7/SocketServer.py", line 310, in process_request self.finish_request(request, client_address) File "/usr/lib/python2.7/SocketServer.py", line 323, in finish_request self.RequestHandlerClass(request, client_address, self) File "/usr/lib/python2.7/SocketServer.py", line 640, in __init__ self.finish() File "/usr/lib/python2.7/SocketServer.py", line 693, in finish self.wfile.flush() File "/usr/lib/python2.7/socket.py", line 303, in flush self._sock.sendall(view[write_offset:write_offset+buffer_size]) error: [Errno 32] Broken pipe 127.0.0.1 -- [19/Sep/2014 05:00:21] "GET /static/js/idfind.js HTTP/1.0" 200 - cloo@pinky:/opt/idfind\$ []
3. cloo@pinky: /opt/idfind (ssh)	System Log	.js HTTP/1.0" 200 - Traceback (most recent call last): File "/usr/lib/python2.7/SocketServer.py", line 284, in _handle_request_no lock self.process_request(request, client_address) File "/usr/lib/python2.7/SocketServer.py", line 310, in process_request self.finish_request(request, client_address) File "/usr/lib/python2.7/SocketServer.py", line 323, in finish_request self.RequestHandlerClass(request, client_address, self) File "/usr/lib/python2.7/SocketServer.py", line 640, in __init__ self.finish() File "/usr/lib/python2.7/SocketServer.py", line 693, in finish self.wfile.flush() File "/usr/lib/python2.7/socket.py", line 303, in flush self._sock.sendall(view[write_offset:write_offset+buffer_size]) error: [Errno 32] Broken pipe 127.0.0.1 -- [19/Sep/2014 05:00:21] "GET /static/js/idfind.js HTTP/1.0" 200 - cloo@pinky:/opt/idfind\$ []
7. cloo@pinky: /var/log (ssh)	System Log	Jun 8 00:03:08 pinky sudo: pam_unix(sudo:session): session closed for user root Jun 8 00:03:09 pinky sshd[32355]: Received disconnect from 104.248.148.6: 11: Bye [preauth] Jun 8 00:03:18 pinky sudo: cloo : TTY=pts/10 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/tail kern.log Jun 8 00:03:18 pinky sudo: pam_unix(sudo:session): session opened for user root by cloo(uid=0) Jun 8 00:03:18 pinky sudo: pam_unix(sudo:session): session closed for user root Jun 8 00:03:25 pinky sudo: cloo : TTY=pts/10 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/tail auth.log Jun 8 00:03:25 pinky sudo: pam_unix(sudo:session): session opened for user root by cloo(uid=0) Jun 8 00:03:25 pinky sudo: pam_unix(sudo:session): session closed for user root Jun 8 00:03:34 pinky sudo: cloo : TTY=pts/10 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/tail -50 auth.log Jun 8 00:03:34 pinky sudo: pam_unix(sudo:session): session opened for user root by cloo(uid=0) cloo@pinky:/var/log\$ []
10. cloo@pinky: /opt/elasticsearch/logs (ssh)	System Log	STATUS wrapper 2018/11/21 15:43:21 http://wrapper.tanukisoftware.org STATUS wrapper 2018/11/21 15:43:21 STATUS wrapper 2018/11/21 15:43:21 Launching a JVM... INFO jvm 1 2018/11/21 15:43:22 WrapperManager: Initializing... STATUS wrapper 2019/04/12 11:37:54 TERM trapped. Shutting down. STATUS wrapper 2019/04/12 11:37:56 <-- Wrapper Stopped STATUS wrapper 2019/04/12 13:06:36 --> Wrapper Started as Daemon STATUS wrapper 2019/04/12 13:06:36 Java Service Wrapper Community Edition 64-bit 3.5.14 STATUS wrapper 2019/04/12 13:06:36 Copyright (C) 1999-2011 Tanuki Software, Ltd. All Rights Reserved. STATUS wrapper 2019/04/12 13:06:36 http://wrapper.tanukisoftware.org STATUS wrapper 2019/04/12 13:06:36 STATUS wrapper 2019/04/12 13:06:36 Launching a JVM... INFO jvm 1 2019/04/12 13:06:36 WrapperManager: Initializing... cloo@pinky:/opt/elasticsearch/logs\$ []



@emanuil_tolev

Well, this is getting challenging
to manage



 elastic

@emanuil_tolev

Very challenging

Search for infrastructure data... (e.g. host.name:host-1)

Hosts

Kubernetes

Docker

Metric: CPU Usage ▾

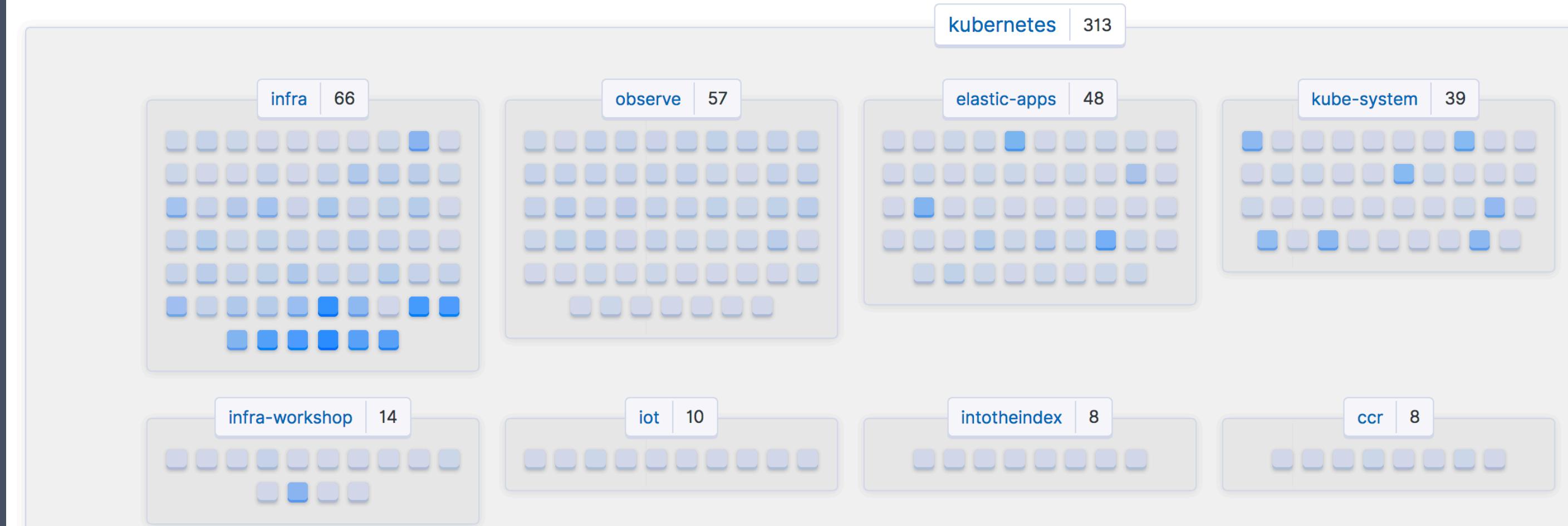
Group By: Service Type Namespace ▾

Configuration

Map View

Table View

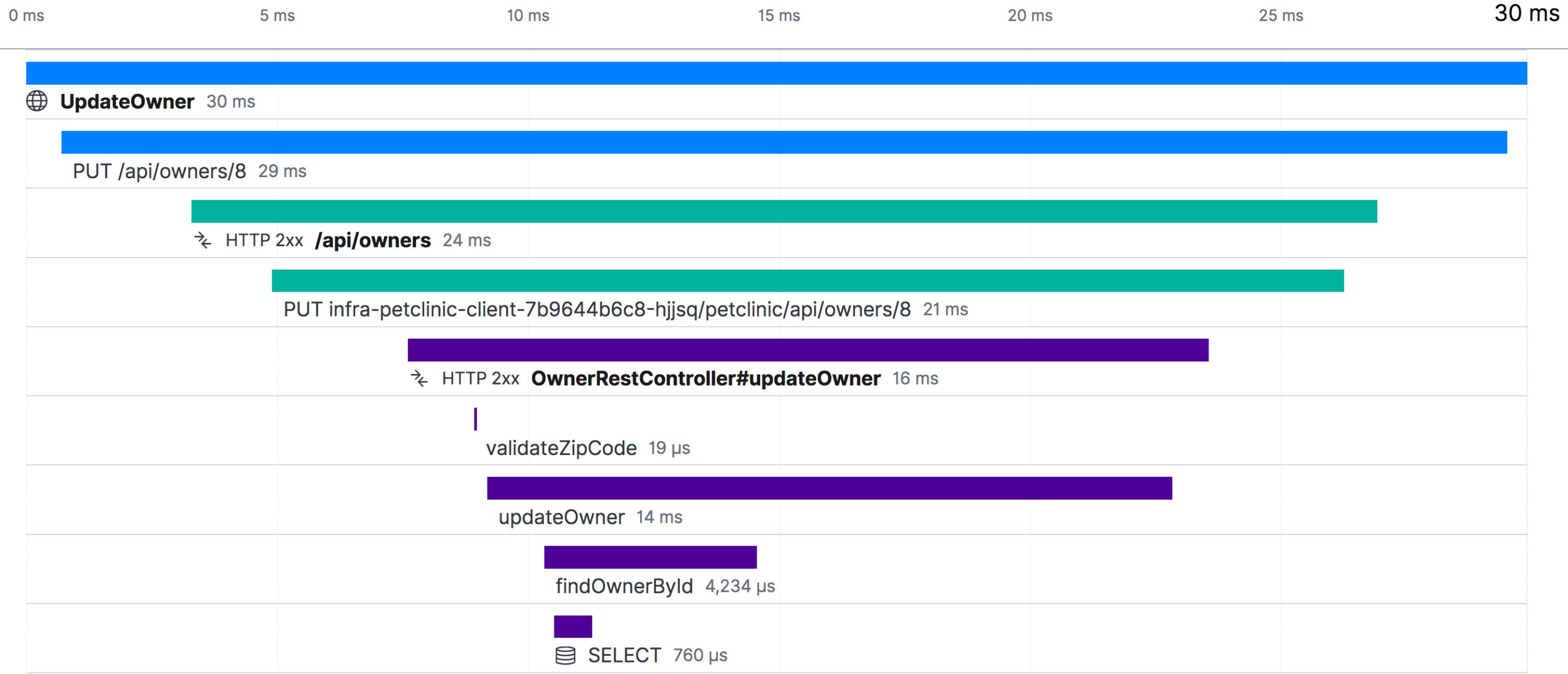
Show



@emanuil_tolev

metrics

Services petclinic-react petclinic-node petclinic-spring



elastic

@emanuil_tolev

apm

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



@emanuil_tolev

Personal story of managing logs and evolving systems

NOW:

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



@emanuil_tolev

Elastic is adding security.

1,021 4 5 3 2

Total Attacks

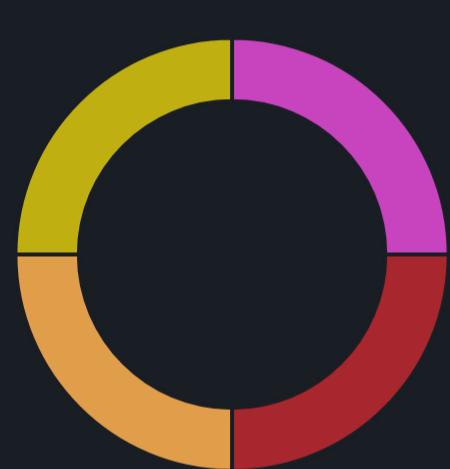
Unique Rules Hit

Unique Sources

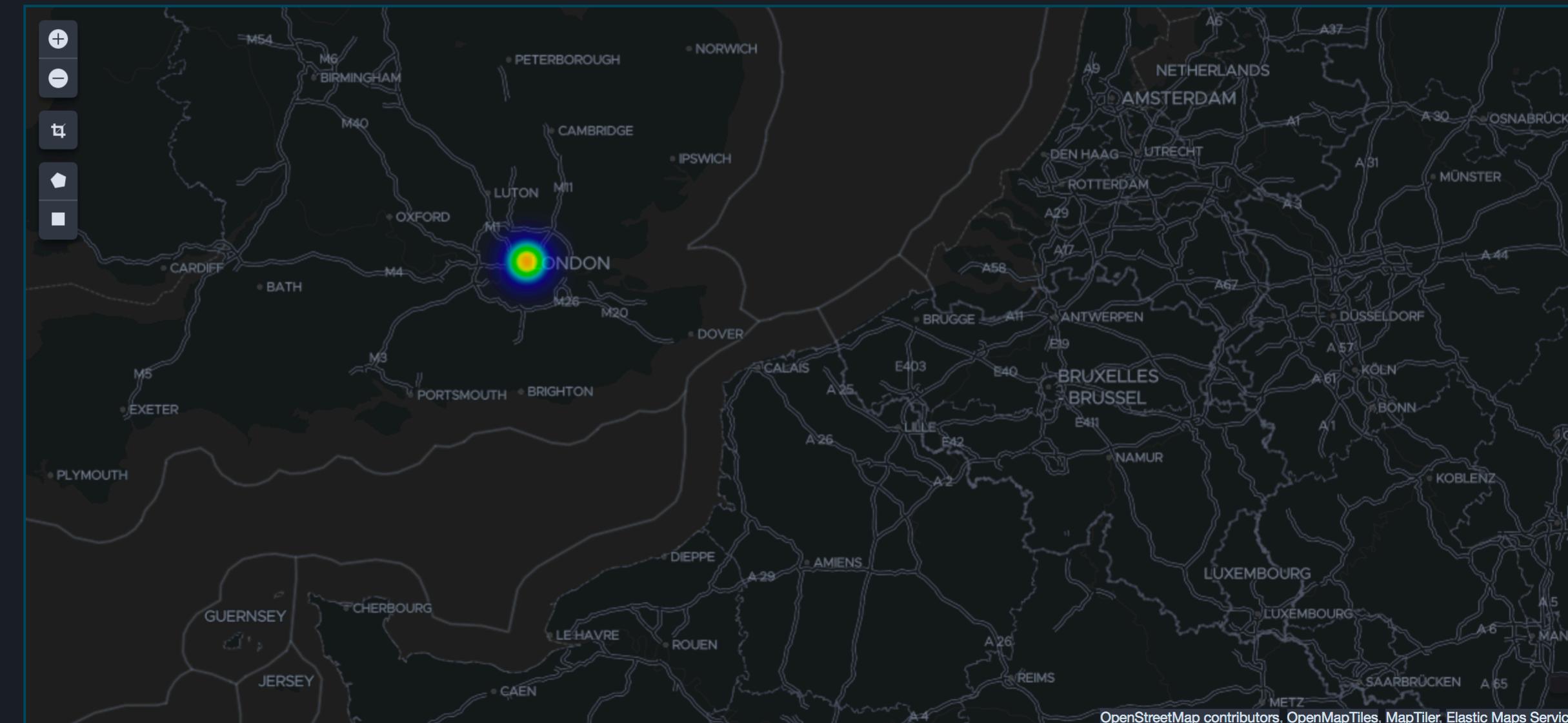
Source Attack Countries

Reporting Hosts

WAF - Chart of Top 10 Rules



WAF - Attack Heat Map



WAF - Chart Of Severities



@emanuil_tolev

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](#)



@emanuil_tolev

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

OBSERVABILITY

[HTTPS://WWW.HONEYCOMB.IO/BLOG/OBSERVABILITY-A-MANIFESTO/](https://www.honeycomb.io/blog/observability-a-manifesto/)



@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"

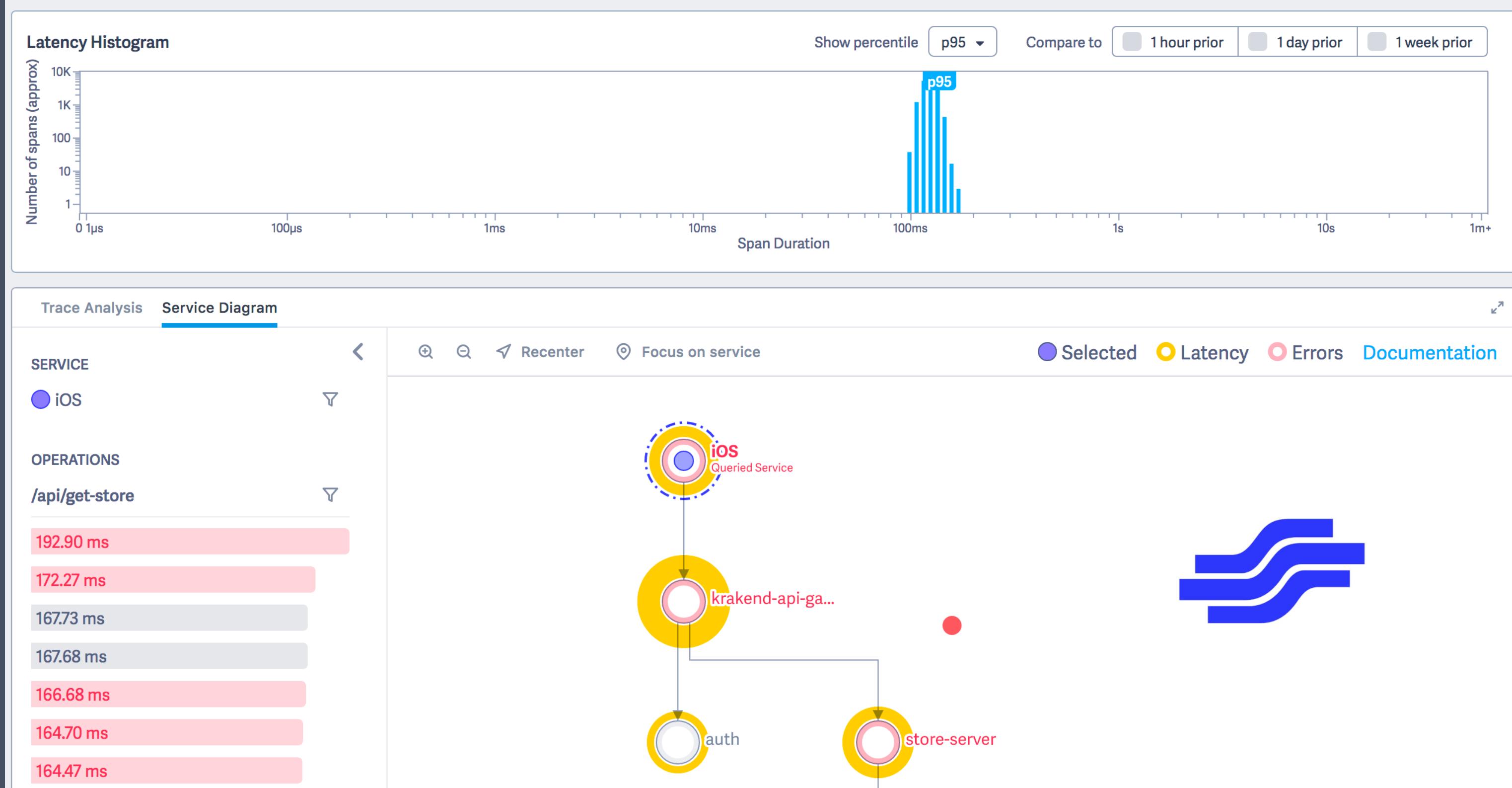
^ "Monitoring is about known-unknowns and actionable alerts, observability is about unknown-unknowns and empowering you to ask arbitrary new questions and explore where the cookie crumbs take you. Observability means you can understand how your systems are working on the inside just by asking questions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

PRESENT INNOVATION

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

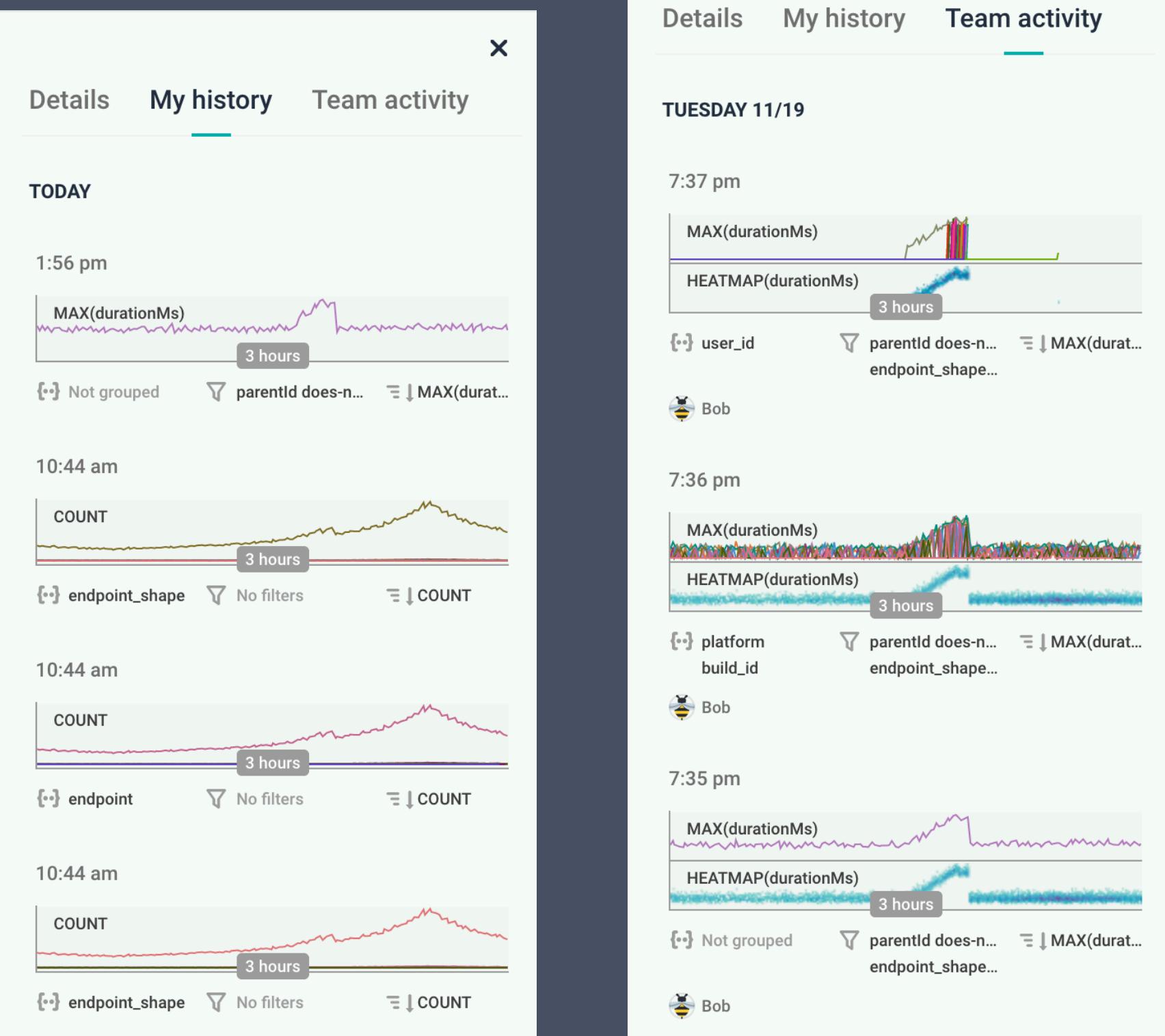


@emanuil_tolev



@emanuil_tolev

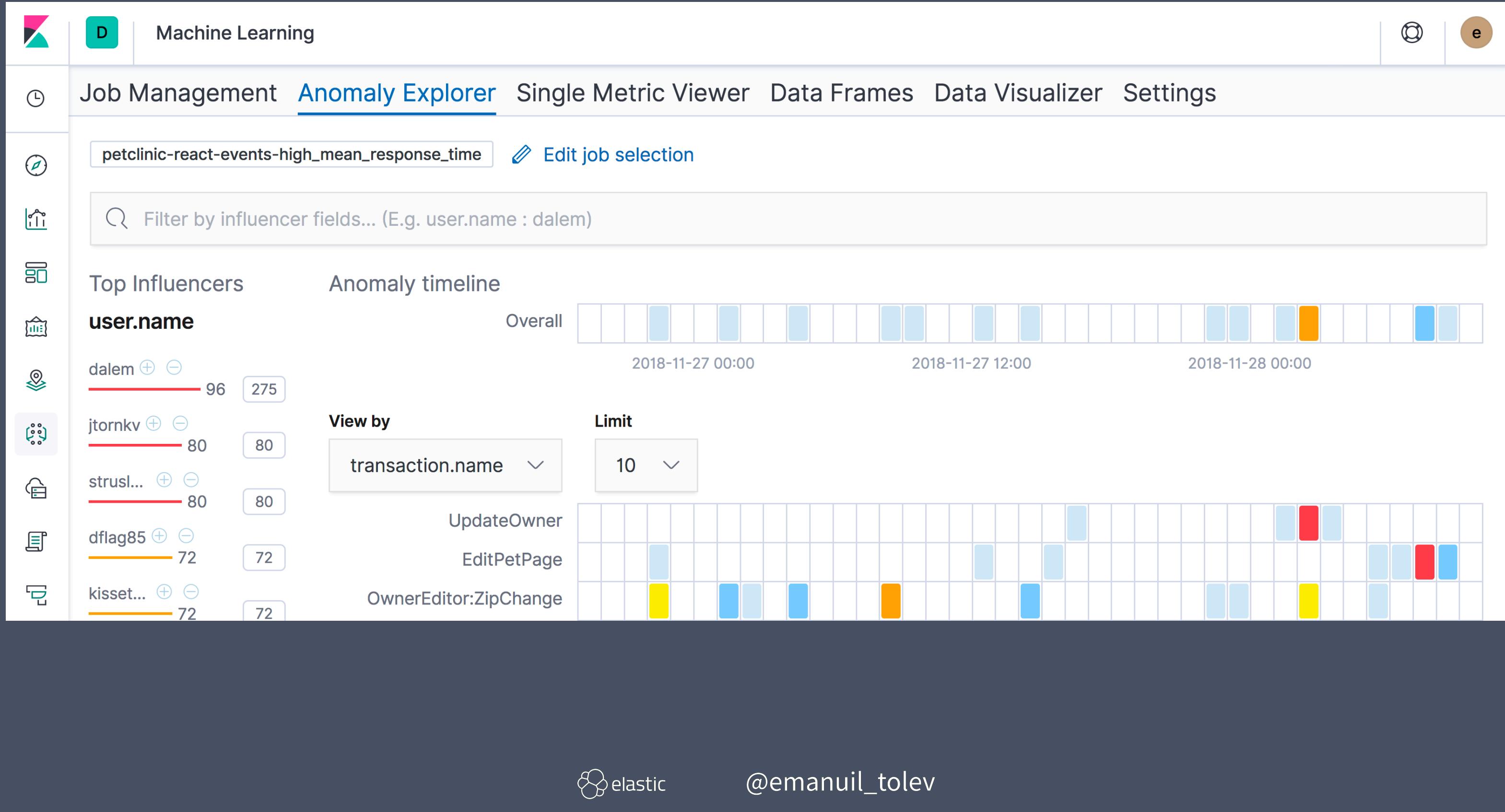
Kind of hard to explain but basically it's a service diagram like you would see in Newrelic and Datadog etc. but. This one overlays the deepest layer (furthest back) at which a specific error is detected. This screenshot shows trying to diagnose a specific problem, it's from their public demo.



elastic

@emanuil_tolev

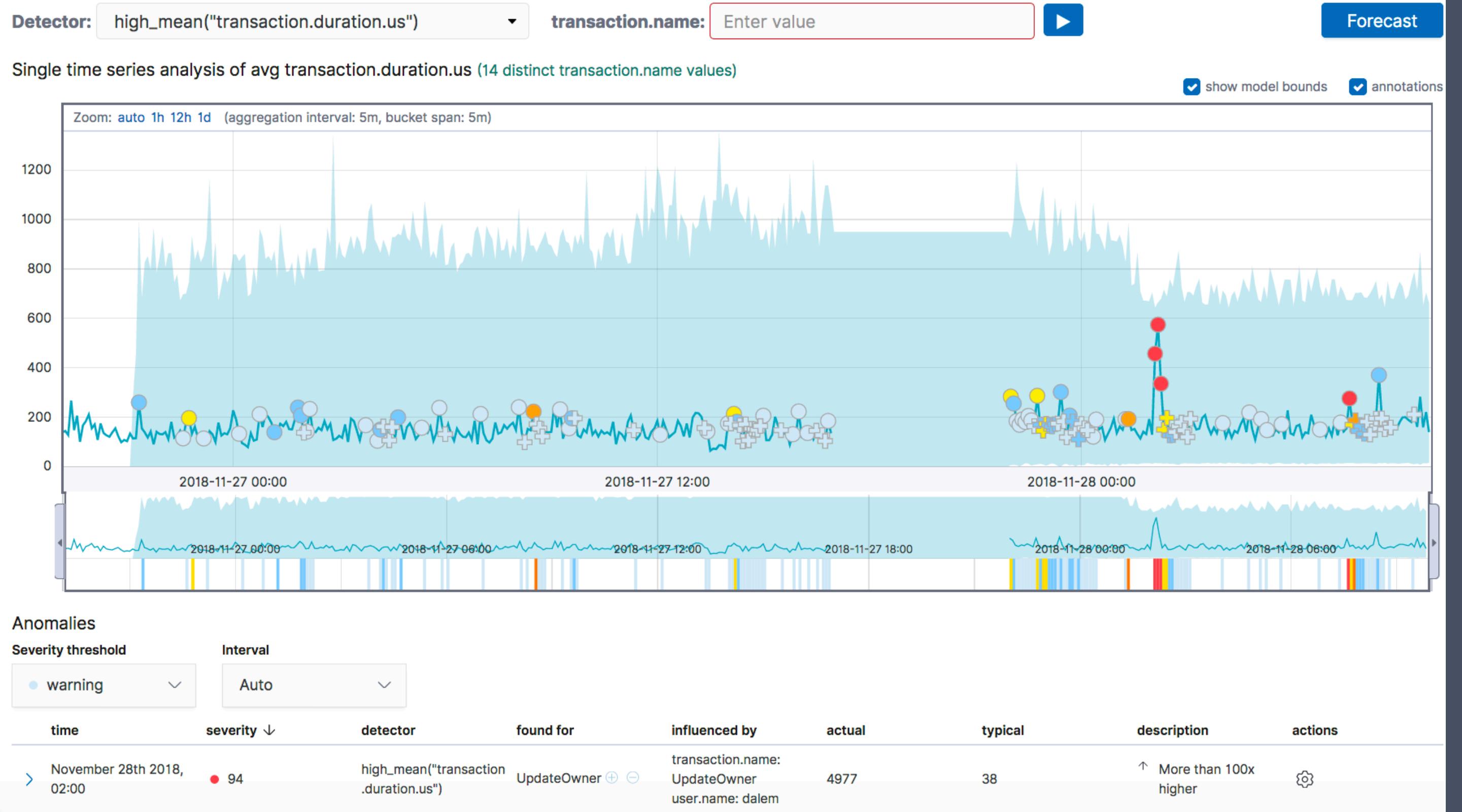
Shows what you yourself looked at – useful at retro. Shows what other ppl looked at – collaborative. Encapsulates team knowledge. An advanced version could be used for training juniors? Writing disaster recovery playbooks straight in your troubleshooting tool?



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.



@emanuil_tolev

a view of the model

BUSINESS MODELS

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



@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



@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!



@emanuil_tolev

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