elastic

Log Management und SIEM in Elastic

Markus Klose | Solution Architect

10.04.2019

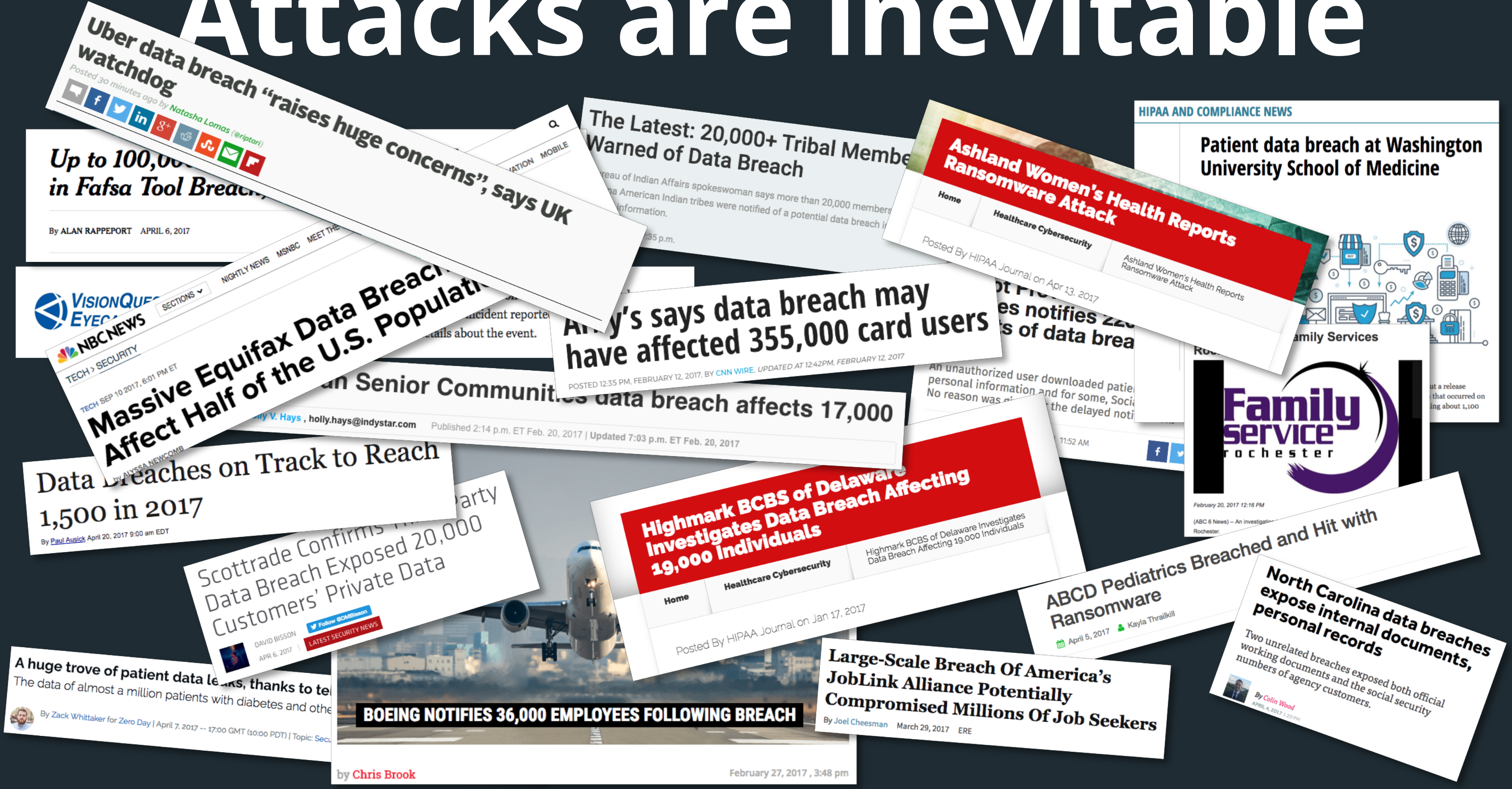
Markus Klose
Solutions Architect
Elastic

Agenda

- Security Analytics mit Elastic
- Observability
- Demo
- Q & A

Security Analytics in Elastic

Attacks are inevitable



Uber data breach "raises huge concerns", says UK watchdog

Posted 30 minutes ago by Natasha Lomas (@riptari)

Up to 100,00 in Fafsa Tool Breach

By ALAN RAPPEPORT APRIL 6, 2017

The Latest: 20,000+ Tribal Membe Warned of Data Breach

reau of Indian Affairs spokeswoman says more than 20,000 members a American Indian tribes were notified of a potential data breach i information.

:35 p.m.

Ashland Women's Health Reports Ransomware Attack

Home | Healthcare Cybersecurity | Ashland Women's Health Reports Ransomware Attack

Posted By HIPAA Journal on Apr 13, 2017

HIPAA AND COMPLIANCE NEWS

Patient data breach at Washington University School of Medicine

VisionQue EyeC

incident reporte tails about the event.

NBC NEWS SECTIONS NIGHTLY NEWS MSNBC MEET THE ATION MOBILE

TECH › SECURITY

TECH SEP 10 2017, 6:01 PM ET

Massive Equifax Data Breach Affect Half of the U.S. Populati

by ALYSSA NEWCOMB

A y's says data breach may have affected 355,000 card users

POSTED 12:35 PM, FEBRUARY 12, 2017, BY CNN WIRE, UPDATED AT 12:42PM, FEBRUARY 12, 2017

ot Pro es notifies 22 ts of data brea

An unauthorized user downloaded patie personal information and for some, Soci No reason was gi the delayed noti

11:52 AM

amily Services

Ro

Family service rochester

February 20, 2017 12:16 PM

(ABC 6 News) -- An investigatio Rochester.

ut a release that occurred on ing about 1,100

an Senior Communit data breach affects 17,000

lly V. Hays , holly.hays@indystar.com Published 2:14 p.m. ET Feb. 20, 2017 | Updated 7:03 p.m. ET Feb. 20, 2017

Data Breaches on Track to Reach 1,500 in 2017

By Paul Ausick April 20, 2017 9:00 am EDT

Scottrade Confirms Th arty Data Breach Exposed 20,000 Customers' Private Data

DAVID BISSON APR 6, 2017 Follow @DMBisson LATEST SECURITY NEWS

Highmark BCBS of Delaware Investigates Data Breach Affecting 19,000 Individuals

Home | Healthcare Cybersecurity | Highmark BCBS of Delaware Investigates Data Breach Affecting 19,000 Individuals

Posted By HIPAA Journal on Jan 17, 2017

ABCD Pediatrics Breached and Hit with Ransomware

April 5, 2017 Kayla Thrailkill

North Carolina data breaches expose internal documents, personal records

Two unrelated breaches exposed both official working documents and the social security numbers of agency customers.

By Colin Wood APRIL 4, 2017 1:20 PM

A huge trove of patient data le ks, thanks to te

The data of almost a million patients with diabetes and othe

By Zack Whittaker for Zero Day | April 7, 2017 -- 17:00 GMT (10:00 PDT) | Topic: Secu

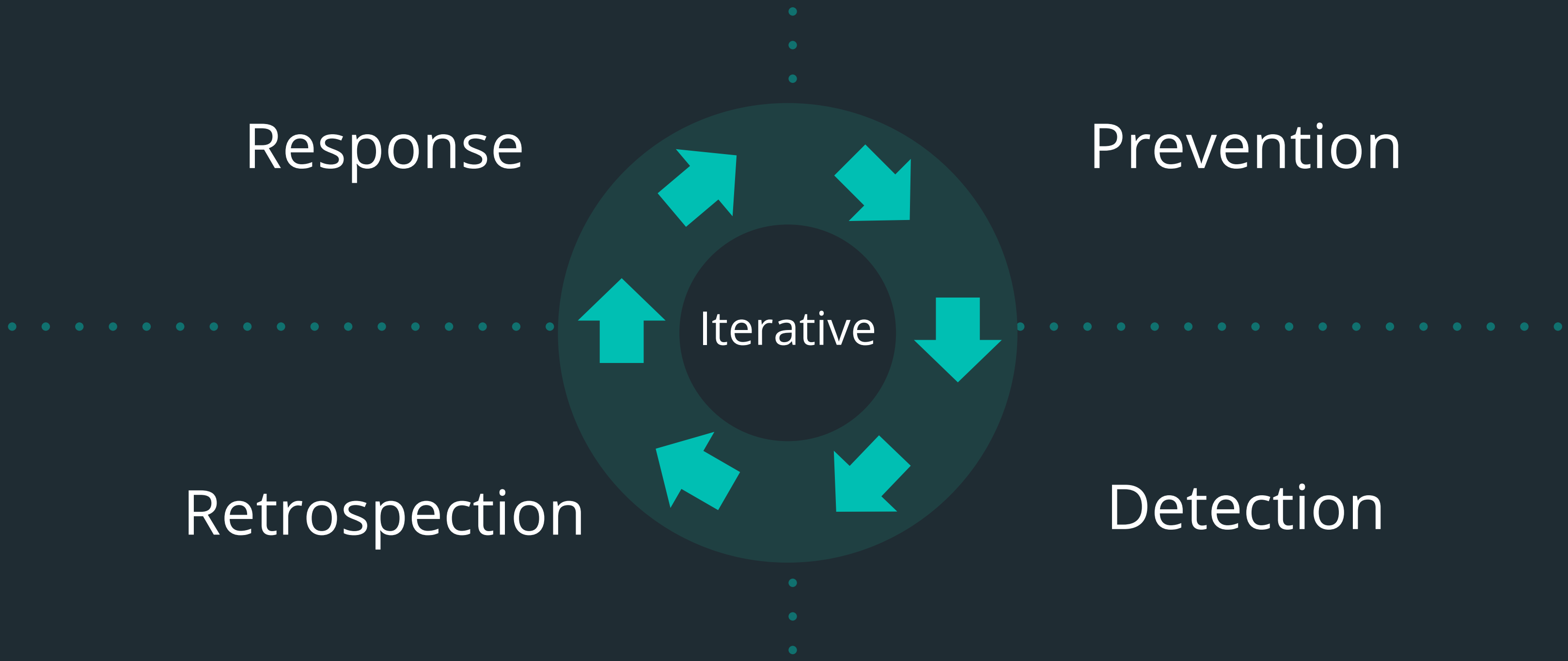
BOEING NOTIFIES 36,000 EMPLOYEES FOLLOWING BREACH

by Chris Brook February 27, 2017 , 3:48 pm

Large-Scale Breach Of America's JobLink Alliance Potentially Compromised Millions Of Job Seekers

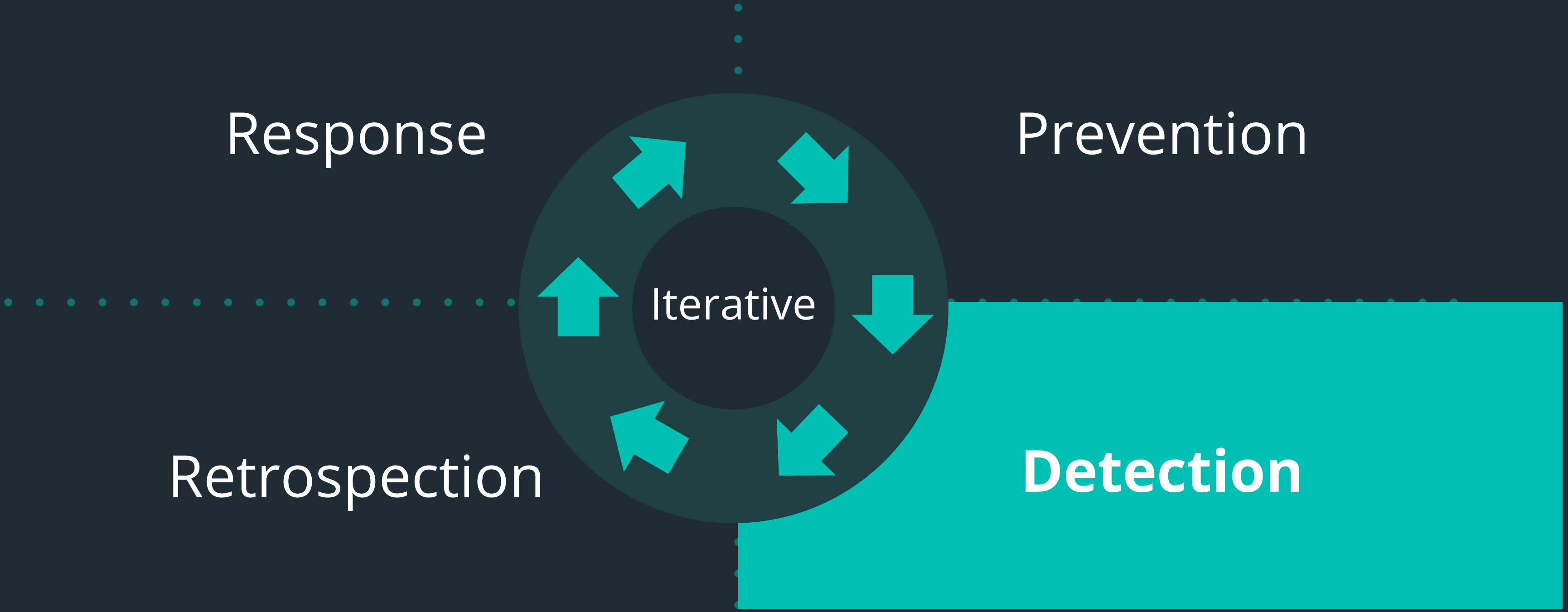
By Joel Cheesman March 29, 2017 ERE

Security is challenging



Prevention falls short

Security is challenging



Response

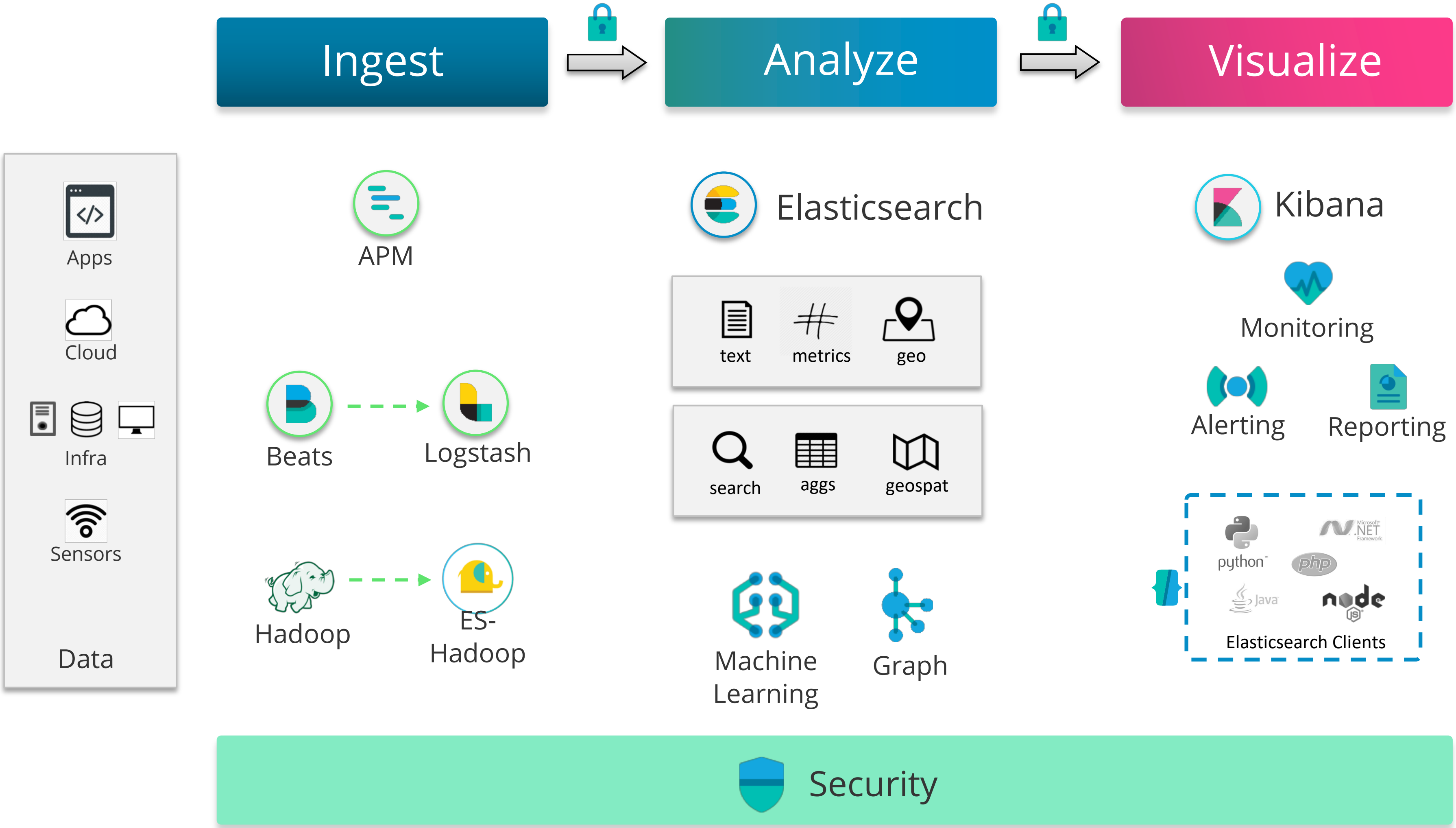
Prevention

Iterative

Retrospection

Detection

Detection is crucial



Ingest

Analyze

Visualize

Apps

Cloud

Infra

Sensors

Data

APM

Beats

Logstash

Hadoop

ES-Hadoop

Elasticsearch

text

metrics

geo

search

aggs

geospat

Machine Learning

Graph

Kibana

Monitoring

Alerting

Reporting

Elasticsearch Clients

Security

What Are Beats?

Lightweight data shippers for *nix systems, macOS and Windows

Winlogbeat
Windows events
AD activity
Remote desktop
Windows FW
Sysmon integ
inc MSSQL…

Auditbeat
Unix audit daemon
File integrity
Processes & users
Monitor anything!

Packetbeat
Traffic (I/O)
Processes
TLS
HTTP payloads
DNS

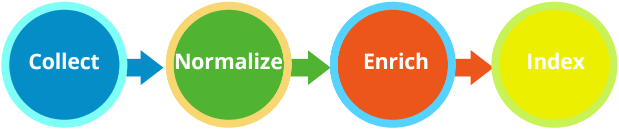
Metricbeat
Metrics
Processes
State of services
PaaS modules

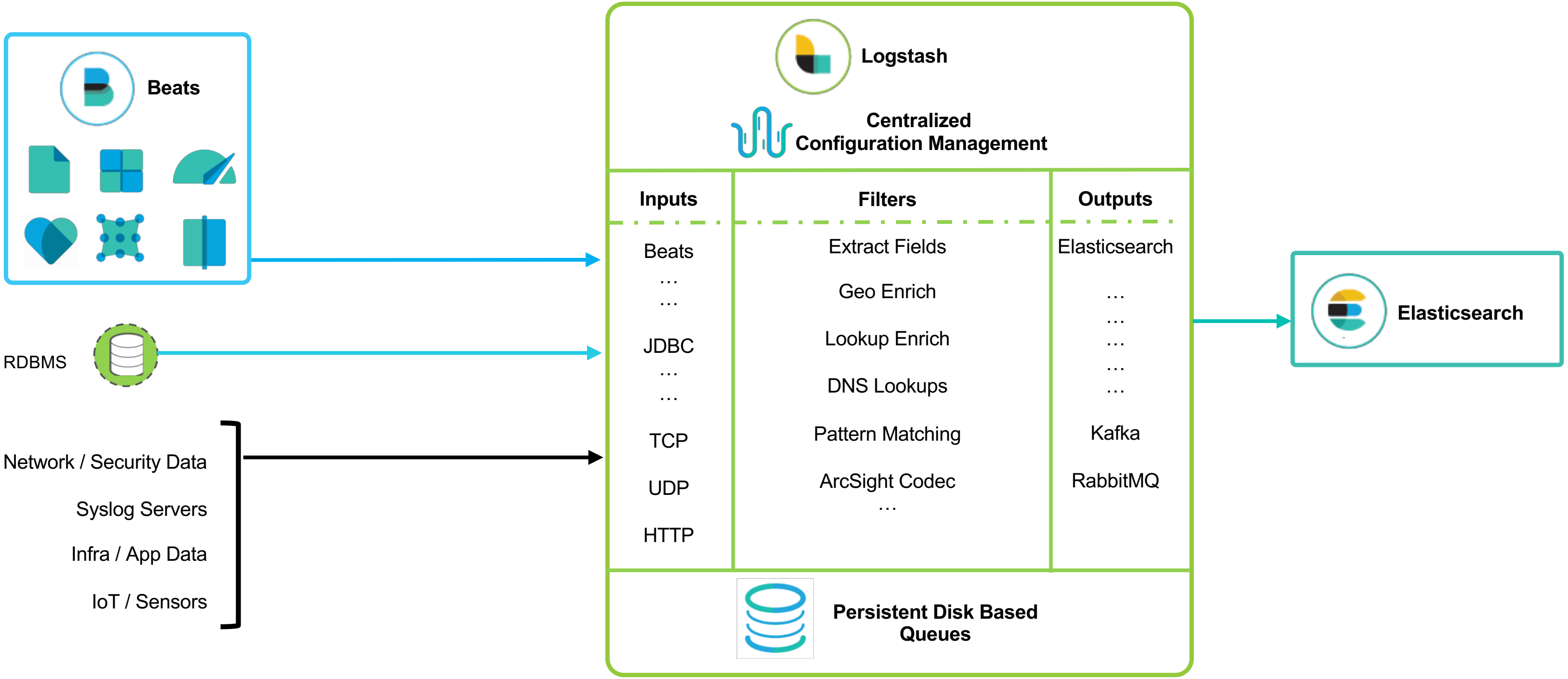
Heartbeat
TCP/UDP
ICMP
HTTP
Expired TLS

Filebeat
File shipper
Osquery integ

Normalization and Enrichment

Using Logstash





Modules

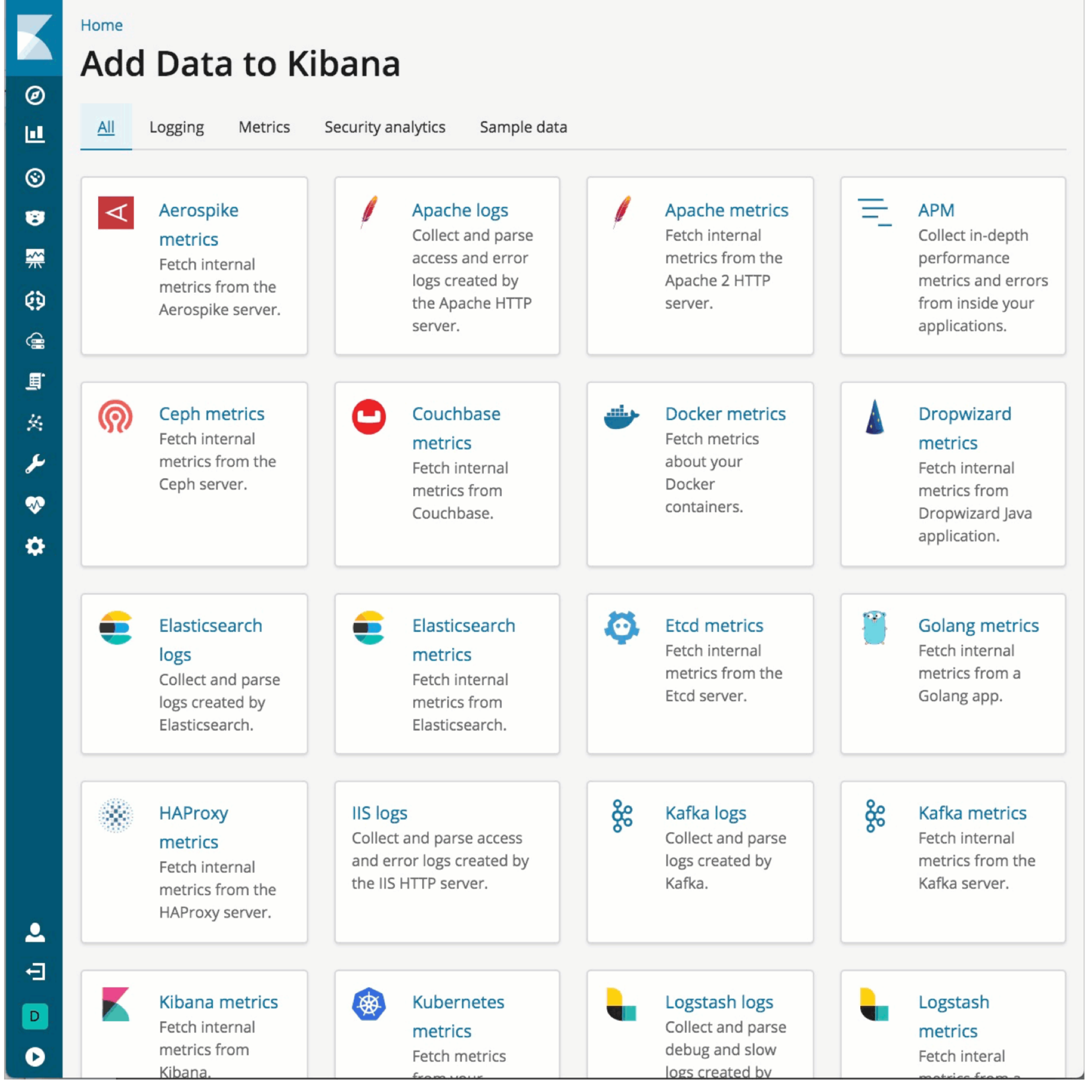
Data to dashboards in 5 minutes

Turnkey for many formats

Automated data parsing

Out of the box dashboards

Preconfigured ML jobs



Add Data to Kibana

Aerospike metrics
Fetch internal metrics from the Aerospike server.

Apache logs
Collect and parse access and error logs created by the Apache HTTP server.

Apache metrics
Fetch internal metrics from the Apache 2 HTTP server.

APM
Collect in-depth performance metrics and errors from inside your applications.

Ceph metrics
Fetch internal metrics from the Ceph server.

Couchbase metrics
Fetch internal metrics from Couchbase.

Docker metrics
Fetch metrics about your Docker containers.

Dropwizard metrics
Fetch internal metrics from Dropwizard Java application.

Elasticsearch logs
Collect and parse logs created by Elasticsearch.

Elasticsearch metrics
Fetch internal metrics from Elasticsearch.

Etcd metrics
Fetch internal metrics from the Etcd server.

Golang metrics
Fetch internal metrics from a Golang app.

HAProxy metrics
Fetch internal metrics from the HAProxy server.

IIS logs
Collect and parse access and error logs created by the IIS HTTP server.

Kafka logs
Collect and parse logs created by Kafka.

Kafka metrics
Fetch internal metrics from the Kafka server.

Kibana metrics
Fetch internal metrics from Kibana.

Kubernetes metrics
Fetch metrics

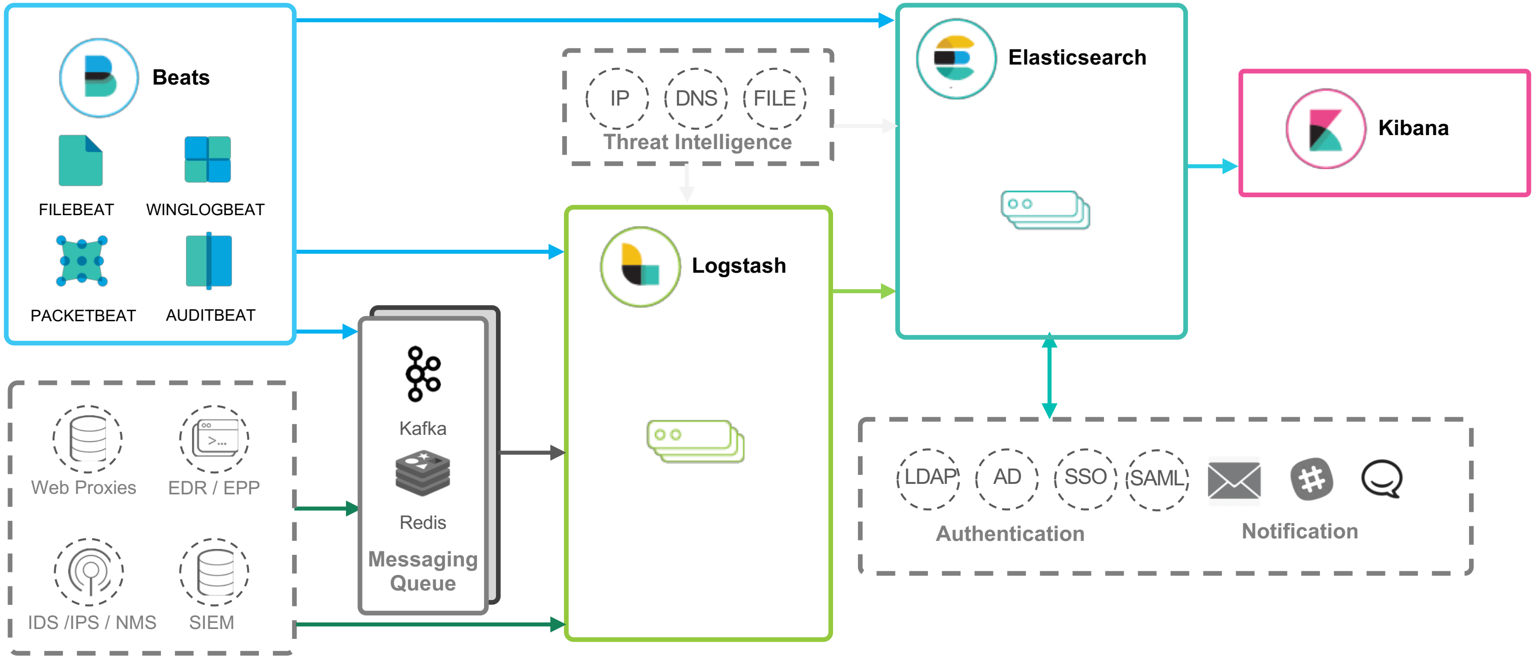
Logstash logs
Collect and parse debug and slow logs created by

Logstash metrics
Fetch interal

Data Sources

Domain	Data Sources	Timing	Tools
Network	PCAP, Bro, NetFlow	Real time, Packet-based	Packetbeats, Logstash (netflow module)
Application	Logs	Real-time, Event-based	Filebeats, Logstash, Sysmon
Cloud	Logs, API	Real-time, Event-based	Beats, Logstash
Host	System State, Signature Alert	Real-time, Asynchronous	Auditbeats, Filebeats (Osquery module), Winlogbeats, Wazuh (HIPS)

Security Analytics Enterprise Architecture



Alerting

Alert on anything you can query

Powered by Elasticsearch

Alert on any Elasticsearch query

Distributed execution

Highly available

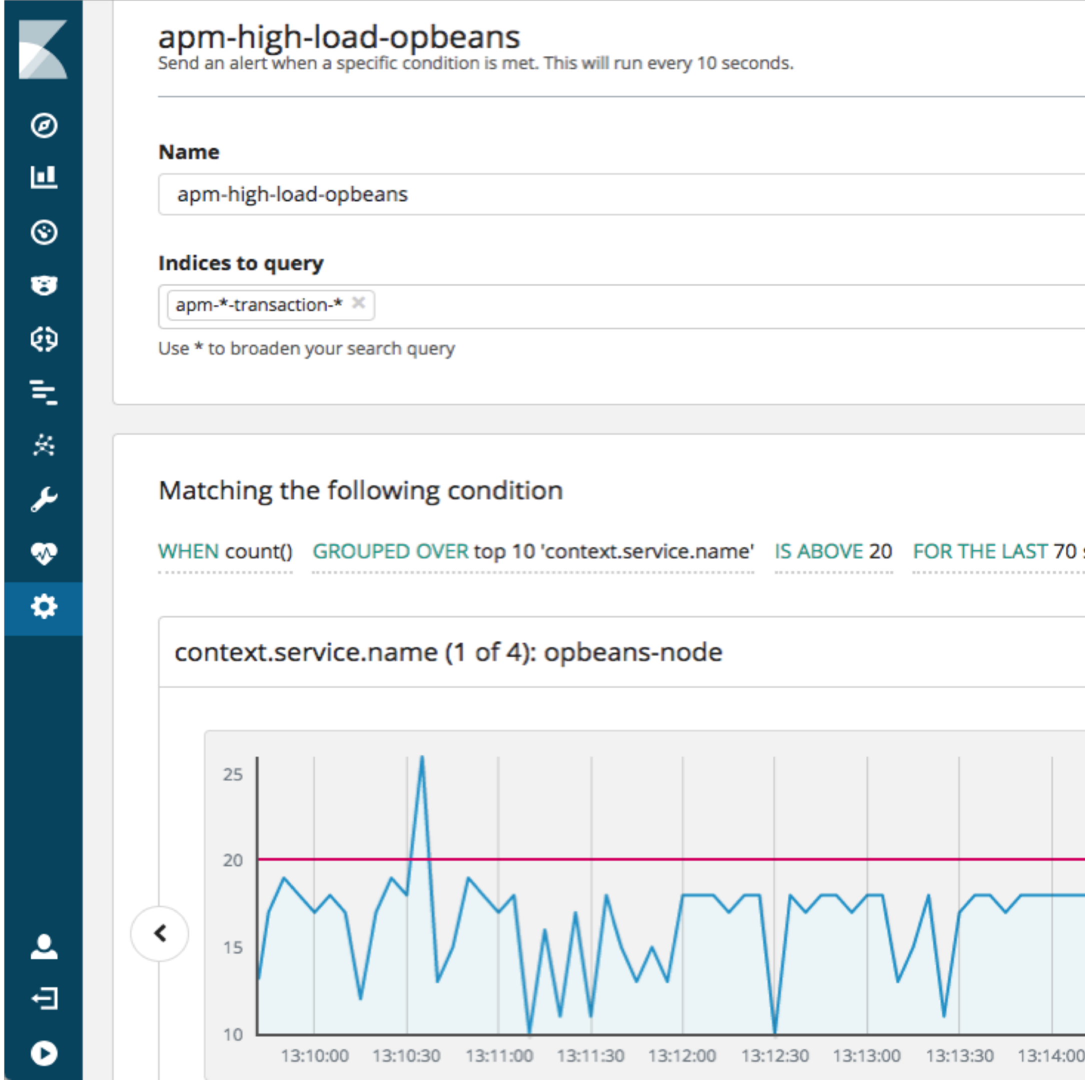
Notifications

Email, Slack, PagerDuty.

Custom (webhook)

Stack Integrations

Machine learning, Monitoring, and Reporting



apm-high-load-opbeans

Send an alert when a specific condition is met. This will run every 10 seconds.

Name

apm-high-load-opbeans

Indices to query

apm-*-transaction-* ✕

Use * to broaden your search query

Matching the following condition

WHEN count() GROUPED OVER top 10 'context.service.name' IS ABOVE 20 FOR THE LAST 70

context.service.name (1 of 4): opbeans-node

Machine Learning

Detect the unusual in your data

Automated Anomaly Detection

Unsupervised algorithms

Continuous (online) model

Single & multiple time series

Population outliers

Forecasting

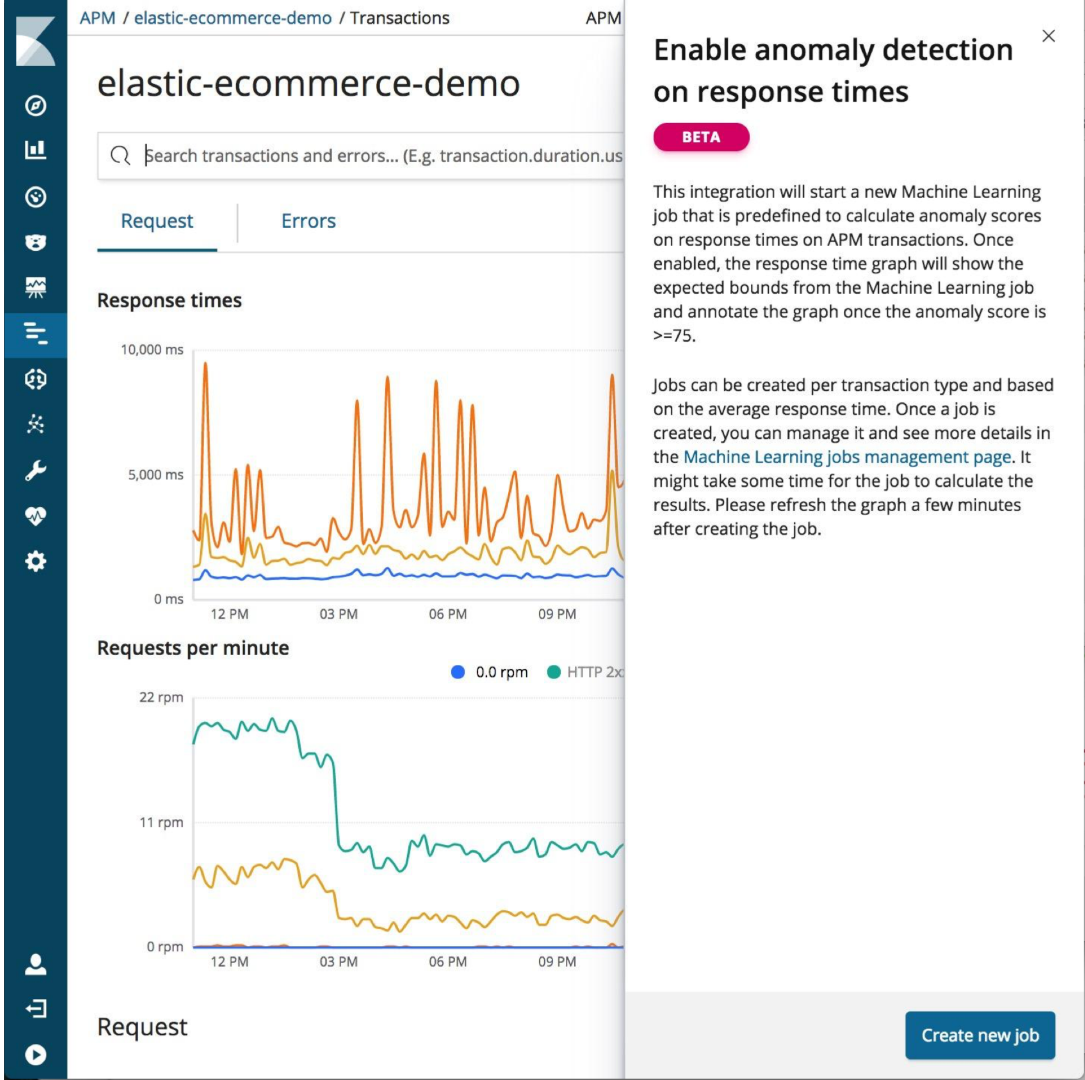
Many Use Cases

IT Operations

Security Analytics

Business KPIs

APM



Enable anomaly detection on response times

BETA

This integration will start a new Machine Learning job that is predefined to calculate anomaly scores on response times on APM transactions. Once enabled, the response time graph will show the expected bounds from the Machine Learning job and annotate the graph once the anomaly score is >=75.

Jobs can be created per transaction type and based on the average response time. Once a job is created, you can manage it and see more details in the Machine Learning jobs management page. It might take some time for the job to calculate the results. Please refresh the graph a few minutes after creating the job.

Graph

Find meaningful connections

Same data. New views.

Uses Elasticsearch relevance features

Includes an API & UI

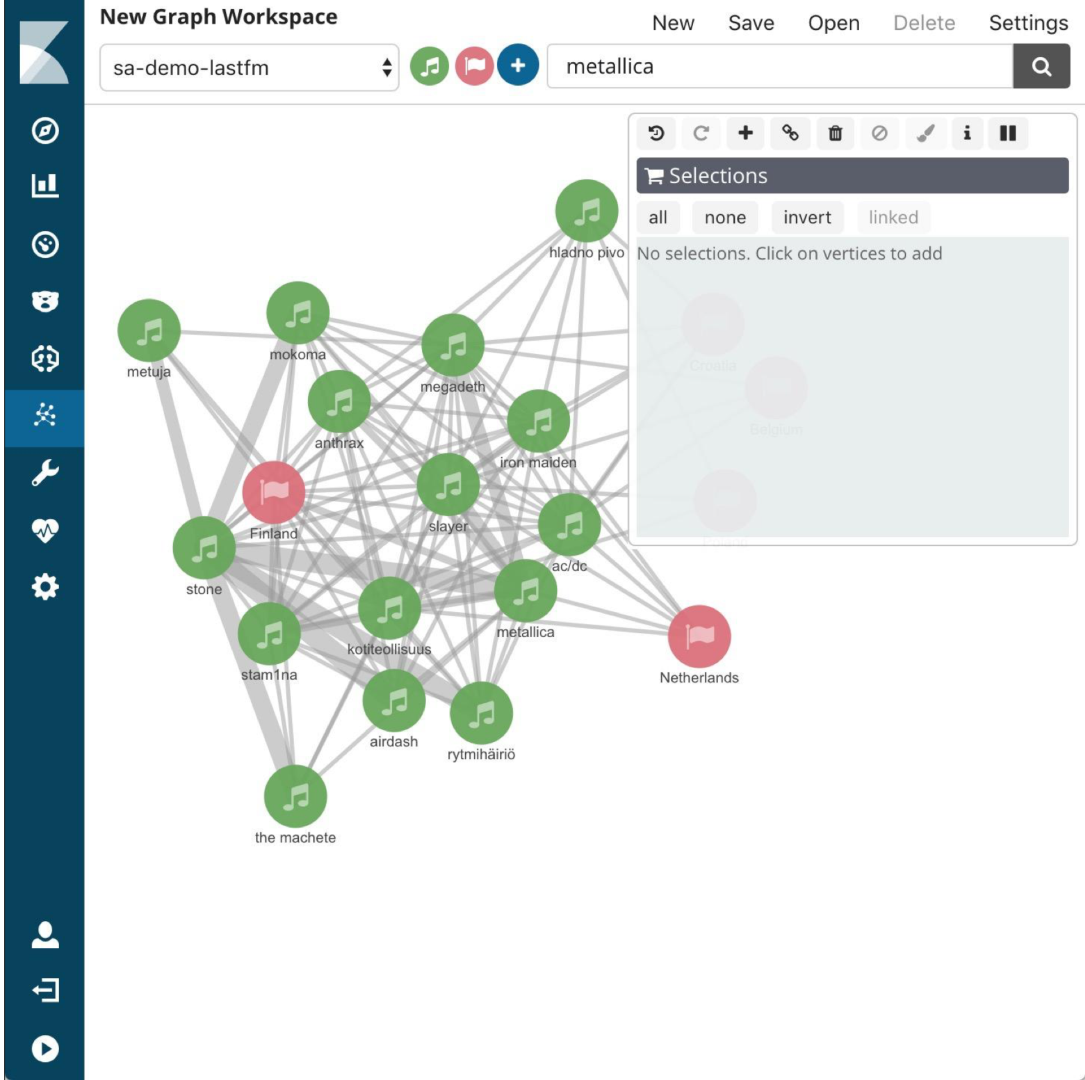
Use Cases

Recommendations

Fraud discovery

Threat hunting

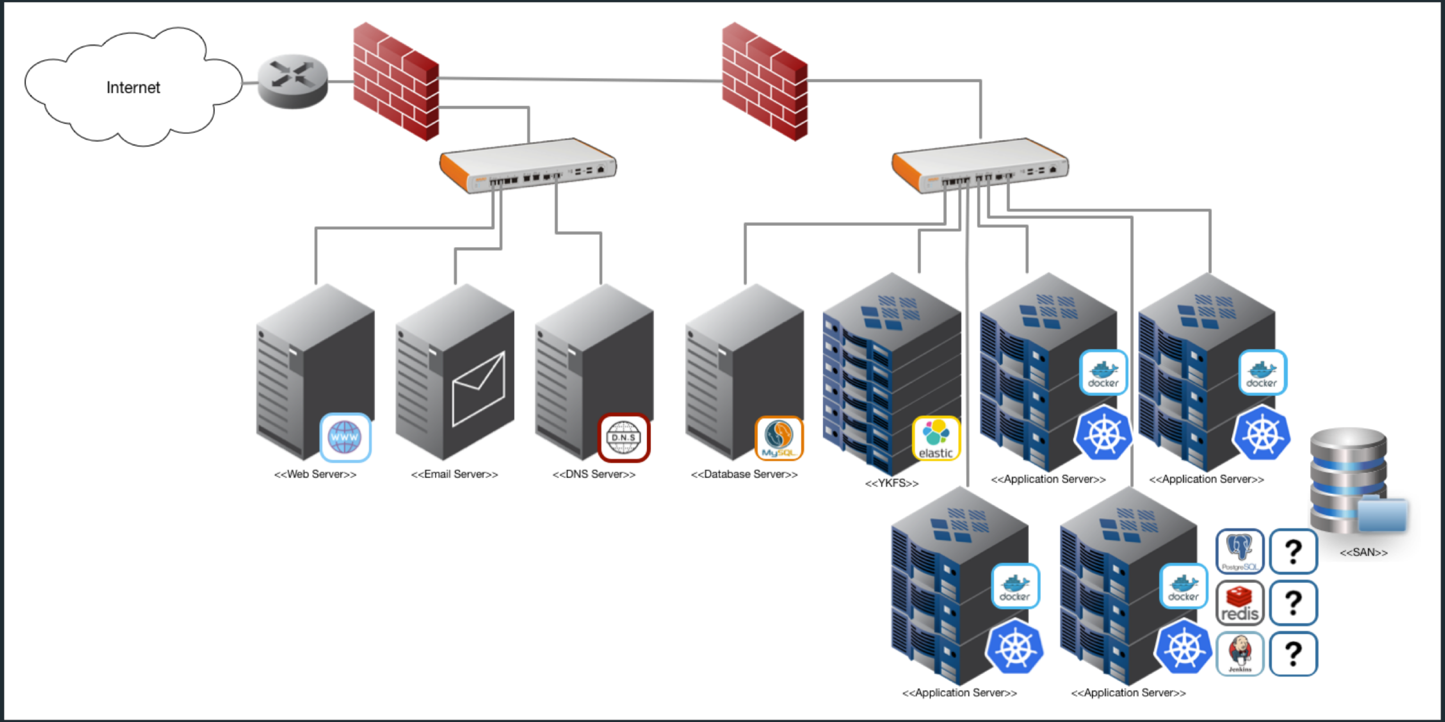
Behavior analysis



Observability

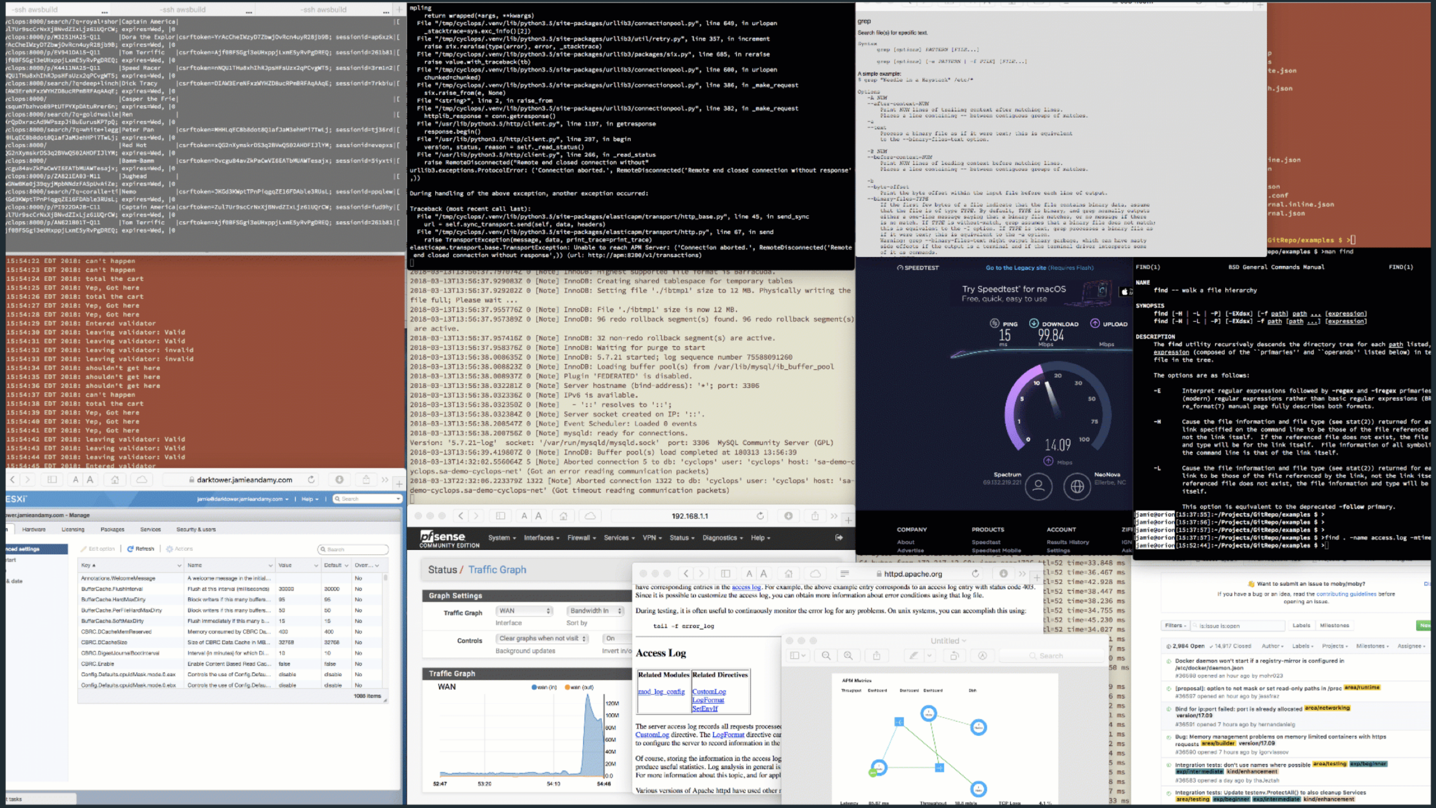
Logging, Metrics and **APM**

You have this ...



.. and when this happens...

you open these...



```
-ssh awsbuild                    -ssh awsbuild                    -ssh awsbuild
yclops:8000/search/?q=royal+shor|Captain America|                                                         |[
ul7Ur9scCrNxXjBNvdZIxLjz61UQrCW; expires=Wed, |0
yclops:8000/p/M3251HA25-Q11      |Dora the Explor|csrftoken=YrAcCheIWzyD7ZbwjOvRcn4uyR28jb9B; sessionid=ap6xzk|[
rAcCheIWzyD7ZbwjOvRcn4uyR28jb9B; expires=Wed, |0
yclops:8000/p/EV941DA15-Q11      |Tom Terrific   |csrftoken=Ajf08FSGgi3eUHxppjLxmE5yRvPgDREQ; sessionid=261b81|[
jf08FSGgi3eUHxppjLxmE5yRvPgDREQ; expires=Wed, |0
yclops:8000/p/K4411NA25-Q11      |Speed Racer    |csrftoken=nNQU1THu8xhIhRJpsHFsUzx2qPCvgWT5; sessionid=3rmln2|[
NQU1THu8xhIhRJpsHFsUzx2qPCvgWT5; expires=Wed, |0
yclops:8000/search/?q=deep+linch|Dick Tracy     |csrftoken=DIAW3EreNFxzWYHZD8ucRPmBRFAqAAqE; sessionid=7rkbiu|[
IAW3EreNFxzWYHZD8ucRPmBRFAqAAqE; expires=Wed, |0
yclops:8000/                     |Casper the Frie|                                                         |[
xsqum7bzhvo69PtUTPYXpDAtuRrer6n; expires=Wed, |0
yclops:8000/search/?q=gold+walle|Ren            |                                                         |[
XrQpDxracAd9WPszpJiBuEurusKP7pQ; expires=Wed, |0
yclops:8000/search/?q=white+legg|Peter Pan      |csrftoken=MHHLqECBb8dot8QlafJaM3ehHPi7TwLj; sessionid=tj36rd|[
HHLqECBb8dot8QlafJaM3ehHPi7TwLj; expires=Wed, |0
yclops:8000/                     |Red Hot        |csrftoken=xQG2nXymskrDS3q2BVwQ502AHDFIJlYM; sessionid=evepxs|[
QG2nXymskrDS3q2BVwQ502AHDFIJlYM; expires=Wed, |0
yclops:8000/                     |Bamm-Bamm      |csrftoken=Dvcgu84avZkPaCwVI6EATbMUAWTesajx; sessionid=5iyxti|[
vcgu84avZkPaCwVI6EATbMUAWTesajx; expires=Wed, |0
yclops:8000/p/ZA821EA03-M11      |Jughead        |                                                         |[
wGNw8Ke0j39qyjMpbNNdzFASpUvAiZe; expires=Wed, |0
yclops:8000/search/?q=coralle+ti|Nemo           |csrftoken=JKGd3KWptTPnPiqgqZE16FDAble3RUsL; sessionid=ppqlew|[
KGd3KWptTPnPiqgqZE16FDAble3RUsL; expires=Wed, |0
yclops:8000/p/PI922DA2B-C11      |Captain America|csrftoken=Zul7Ur9scCrNxXjBNvdZIxLjz61UQrCW; sessionid=fud9hy|[
ul7Ur9scCrNxXjBNvdZIxLjz61UQrCW; expires=Wed, |0
yclops:8000/p/AN621B01T-Q11      |Tom Terrific   |csrftoken=Ajf08FSGgi3eUHxppjLxmE5yRvPgDREQ; sessionid=261b81|[
jf08FSGgi3eUHxppjLxmE5yRvPgDREQ; expires=Wed, |0
```

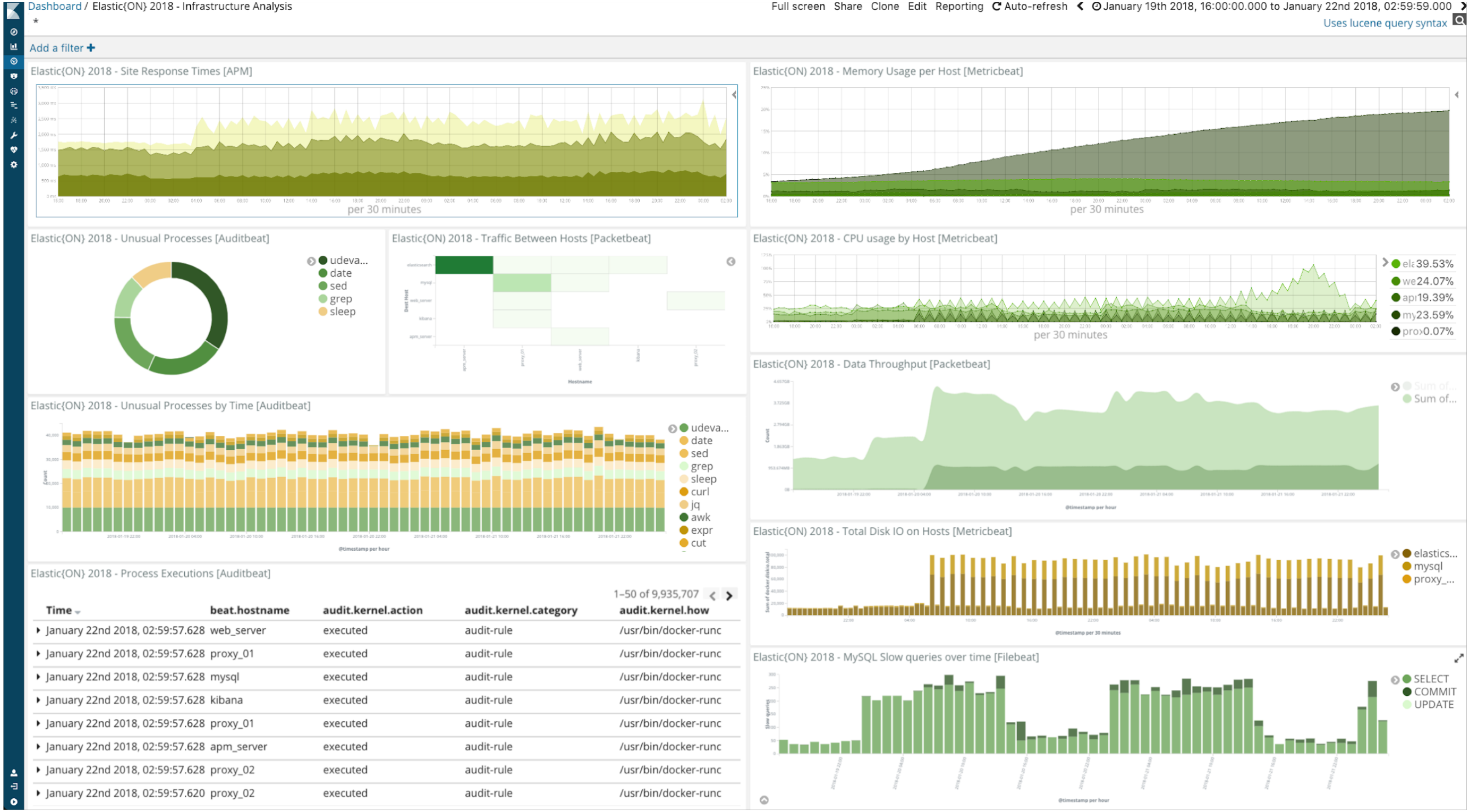
```
mpling
    return wrapped(*args, **kwargs)
  File "/tmp/cyclops/.venv/lib/python3.5/site-packages/urllib3/connectionpool.py", line 649, in urlopen
    _stacktrace=sys.exc_info()[2])
  File "/tmp/cyclops/.venv/lib/python3.5/site-packages/urllib3/util/retry.py", line 357, in increment
    raise six.reraise(type(error), error, _stacktrace)
  File "/tmp/cyclops/.venv/lib/python3.5/site-packages/urllib3/packages/six.py", line 685, in reraise
    raise value.with_traceback(tb)
  File "/tmp/cyclops/.venv/lib/python3.5/site-packages/urllib3/connectionpool.py", line 600, in urlopen
    chunked=chunked)
  File "/tmp/cyclops/.venv/lib/python3.5/site-packages/urllib3/connectionpool.py", line 386, in _make_request
    six.raise_from(e, None)
  File "<string>", line 2, in raise_from
  File "/tmp/cyclops/.venv/lib/python3.5/site-packages/urllib3/connectionpool.py", line 382, in _make_request
    httplib_response = conn.getresponse()
  File "/usr/lib/python3.5/http/client.py", line 1197, in getresponse
    response.begin()
  File "/usr/lib/python3.5/http/client.py", line 297, in begin
    version, status, reason = self._read_status()
  File "/usr/lib/python3.5/http/client.py", line 266, in _read_status
    raise RemoteDisconnected("Remote end closed connection without"
urllib3.exceptions.ProtocolError: ('Connection aborted.', RemoteDisconnected('Remote end closed connection without response'
,))

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/tmp/cyclops/.venv/lib/python3.5/site-packages/elasticapm/transport/http_base.py", line 45, in send_sync
    url = self.sync_transport.send(self, data, headers)
  File "/tmp/cyclops/.venv/lib/python3.5/site-packages/elasticapm/transport/http.py", line 67, in send
    raise TransportException(message, data, print_trace=print_trace)
elasticapm.transport.base.TransportException: Unable to reach APM Server: ('Connection aborted.', RemoteDisconnected('Remote
 end closed connection without response',)) (url: http://apm:8200/v1/transactions)
```

```
grep
Search file(s) for specific text.
```

```
15:54:22 EDT 2018: can't happen
15:54:23 EDT 2018: can't happen
15:54:24 EDT 2018: total the cart
15:54:25 EDT 2018: Yep, Got here
15:54:26 EDT 2018: total the cart
15:54:27 EDT 2018: Yep, Got here
15:54:28 EDT 2018: Yep, Got here
15:54:29 EDT 2018: Entered validator
15:54:30 EDT 2018: leaving validator: Valid
15:54:31 EDT 2018: leaving validator: Valid
15:54:32 EDT 2018: leaving validator: invalid
15:54:33 EDT 2018: leaving validator: invalid
15:54:34 EDT 2018: shouldn't get here
15:54:35 EDT 2018: shouldn't get here
15:54:36 EDT 2018: shouldn't get here
15:54:37 EDT 2018: can't happen
15:54:38 EDT 2018: total the cart
15:54:39 EDT 2018: Yep, Got here
15:54:40 EDT 2018: Yep, Got here
15:54:41 EDT 2018: Yep, Got here
15:54:42 EDT 2018: leaving validator: Valid
15:54:43 EDT 2018: leaving validator: Valid
15:54:44 EDT 2018: leaving validator: Valid
15:54:45 EDT 2018: Entered validator
```

```
2018-03-13T13:56:37.929083Z 0 [Note] InnoDB: Creating shared tablespace for temporary tables
2018-03-13T13:56:37.929282Z 0 [Note] InnoDB: Setting file './ibtmp1' size to 12 MB. Physically writing the
file full; Please wait ...
2018-03-13T13:56:37.955776Z 0 [Note] InnoDB: File './ibtmp1' size is now 12 MB.
2018-03-13T13:56:37.957389Z 0 [Note] InnoDB: 96 redo rollback segment(s) found. 96 redo rollback segment(s)
 are active.
2018-03-13T13:56:37.957416Z 0 [Note] InnoDB: 32 non-redo rollback segment(s) are active.
2018-03-13T13:56:37.958376Z 0 [Note] InnoDB: Waiting for purge to start
2018-03-13T13:56:38.008635Z 0 [Note] InnoDB: 5.7.21 started; log sequence number 75588091260
2018-03-13T13:56:38.008823Z 0 [Note] InnoDB: Loading buffer pool(s) from /var/lib/mysql/ib_buffer_pool
2018-03-13T13:56:38.008937Z 0 [Note] Plugin 'FEDERATED' is disabled.
2018-03-13T13:56:38.032281Z 0 [Note] Server hostname (bind-address): '*'; port: 3306
2018-03-13T13:56:38.032336Z 0 [Note] IPv6 is available.
2018-03-13T13:56:38.032350Z 0 [Note]   - '::' resolves to '::';
2018-03-13T13:56:38.032384Z 0 [Note] Server socket created on IP: '::'.
2018-03-13T13:56:38.208547Z 0 [Note] Event Scheduler: Loaded 0 events
2018-03-13T13:56:38.208756Z 0 [Note] mysqld: ready for connections.
Version: '5.7.21-log'  socket: '/var/run/mysqld/mysqld.sock'  port: 3306  MySQL Community Server (GPL)
2018-03-13T13:56:39.419807Z 0 [Note] InnoDB: Buffer pool(s) load completed at 180313 13:56:39
2018-03-13T14:32:02.556064Z 5 [Note] Aborted connection 5 to db: 'cyclops' user: 'cyclops' host: 'sa-demo-c
yclops.sa-demo-cyclops-net' (Got an error reading communication packets)
2018-03-13T22:32:06.223379Z 1322 [Note] Aborted connection 1322 to db: 'cyclops' user: 'cyclops' host: 'sa-
demo-cyclops.sa-demo-cyclops-net' (Got timeout reading communication packets)
```

```
GitRepo/examples $ >
epo/examples $ >man find

FIND(1)                 BSD General Commands Manual                 FIND(1)

NAME
     find -- walk a file hierarchy

SYNOPSIS
     find [-H | -L | -P] [-EXdsx] [-f path] path ... [expression]
     find [-H | -L | -P] [-EXdsx] -f path [path ...] [expression]

DESCRIPTION
     The find utility recursively descends the directory tree for each path listed,
     expression (composed of the ``primaries'' and ``operands'' listed below) in te
     file in the tree.

     The options are as follows:

     -E      Interpret regular expressions followed by -regex and -iregex primaries
             (modern) regular expressions rather than basic regular expressions (BR
             re_format(7) manual page fully describes both formats.

     -H      Cause the file information and file type (see stat(2)) returned for ea
             link specified on the command line to be those of the file referenced
             not the link itself.  If the referenced file does not exist, the file
             and type will be for the link itself.  File information of all symboli
             the command line is that of the link itself.

     -L      Cause the file information and file type (see stat(2)) returned for ea
             link to be those of the file referenced by the link, not the link itse
             referenced file does not exist, the file information and type will be
             itself.

             This option is equivalent to the deprecated -follow primary.
jamie@orion[15:37:55]:~/Projects/GitRepo/examples $ >
jamie@orion[15:37:56]:~/Projects/GitRepo/examples $ >
jamie@orion[15:37:57]:~/Projects/GitRepo/examples $ >
jamie@orion[15:37:57]:~/Projects/GitRepo/examples $ >find . -name access.log -mtime
jamie@orion[15:52:44]:~/Projects/GitRepo/examples $ >
```



Dashboard / Elastic{ON} 2018 - Infrastructure Analysis *

Full screen Share Clone Edit Reporting Auto-refresh January 19th 2018, 16:00:00.000 to January 22nd 2018, 02:59:59.000

Uses lucene query syntax

Add a filter +

Elastic{ON} 2018 - Site Response Times [APM]

Elastic{ON} 2018 - Memory Usage per Host [Metricbeat]

Elastic{ON} 2018 - Unusual Processes [Auditbeat]

Elastic{ON} 2018 - Traffic Between Hosts [Packetbeat]

Elastic{ON} 2018 - CPU usage by Host [Metricbeat]

Elastic{ON} 2018 - Data Throughput [Packetbeat]

Elastic{ON} 2018 - Unusual Processes by Time [Auditbeat]

Elastic{ON} 2018 - Total Disk IO on Hosts [Metricbeat]

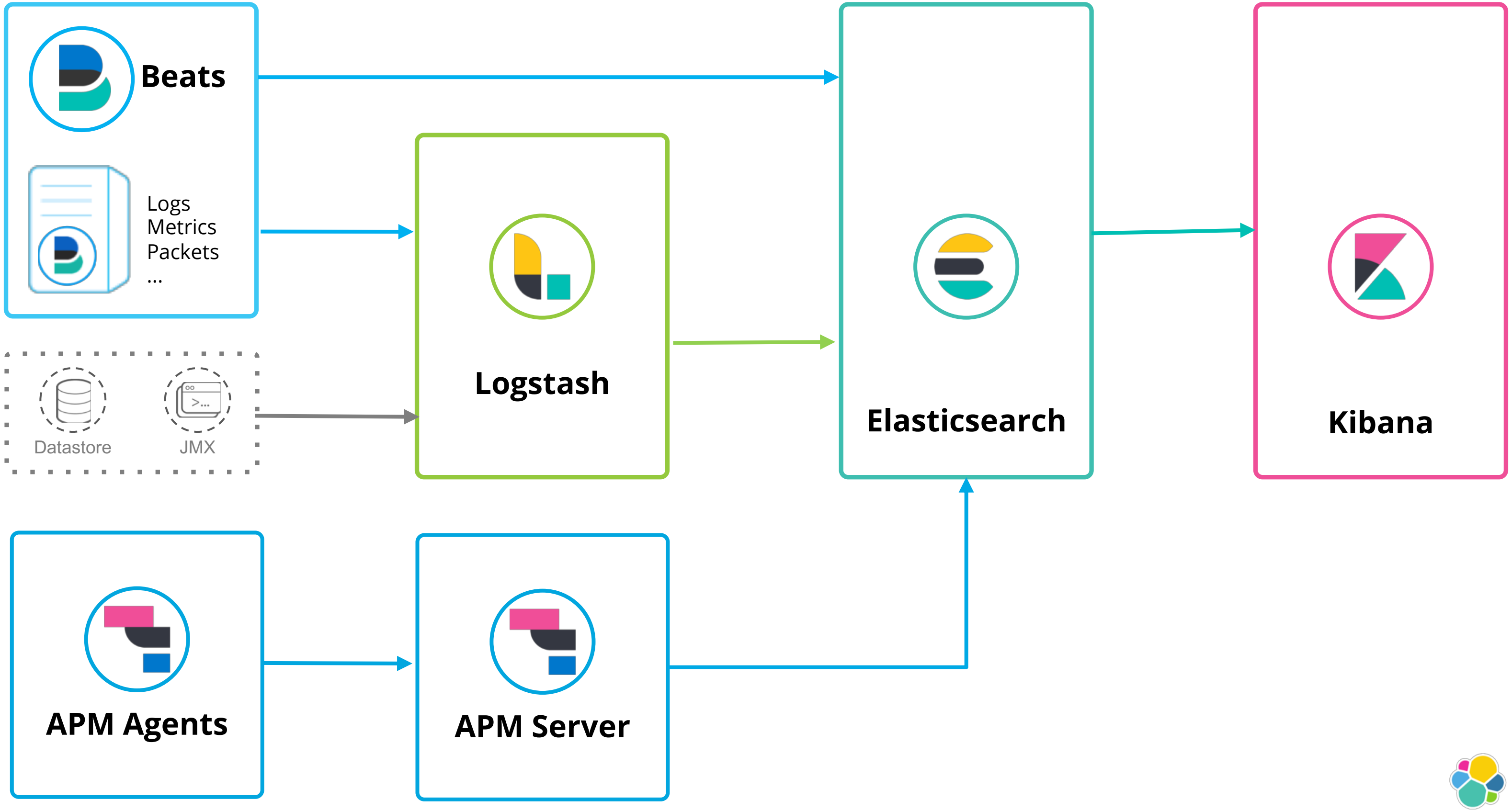
Elastic{ON} 2018 - Process Executions [Auditbeat]

1–50 of 9,935,707

Time	beat.hostname	audit.kernel.action	audit.kernel.category	audit.kernel.how
January 22nd 2018, 02:59:57.628	web_server	executed	audit-rule	/usr/bin/docker-runc
January 22nd 2018, 02:59:57.628	proxy_01	executed	audit-rule	/usr/bin/docker-runc
January 22nd 2018, 02:59:57.628	mysql	executed	audit-rule	/usr/bin/docker-runc
January 22nd 2018, 02:59:57.628	kibana	executed	audit-rule	/usr/bin/docker-runc
January 22nd 2018, 02:59:57.628	proxy_01	executed	audit-rule	/usr/bin/docker-runc
January 22nd 2018, 02:59:57.628	apm_server	executed	audit-rule	/usr/bin/docker-runc
January 22nd 2018, 02:59:57.628	proxy_02	executed	audit-rule	/usr/bin/docker-runc
January 22nd 2018, 02:59:57.620	proxy_02	executed	audit-rule	/usr/bin/docker-runc

Elastic{ON} 2018 - MySQL Slow queries over time [Filebeat]

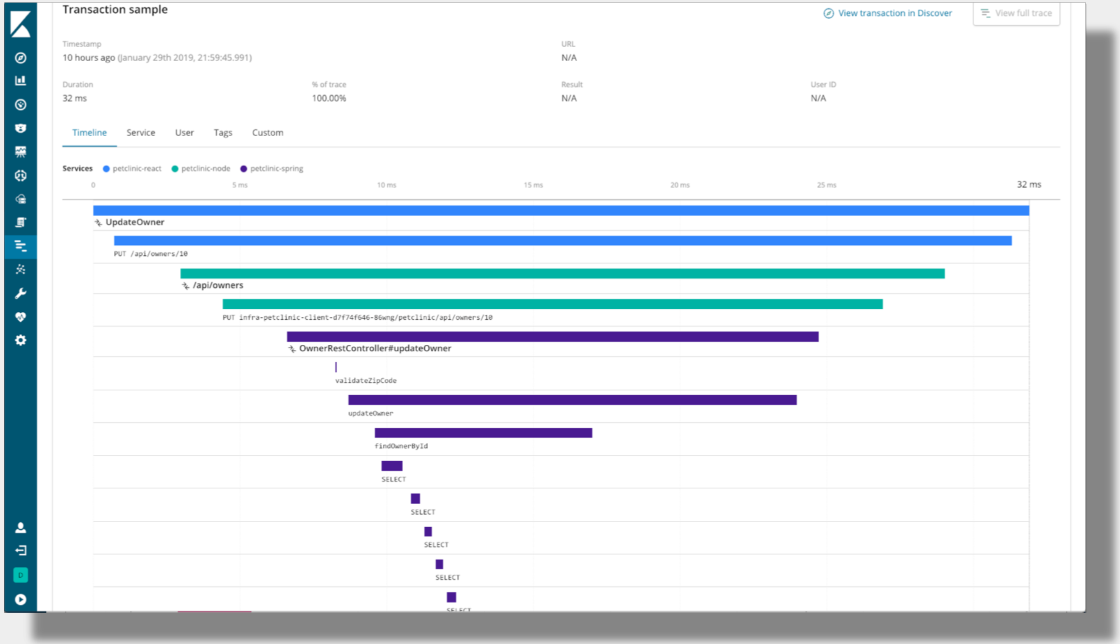
Where APM fits in the Elastic Stack



Track key application metrics

- Response time for requests
- Unhandled errors & exceptions
- Visualize call hierarchy (waterfall chart)
- Identify code bottlenecks
- Drill down to the code level

Distributed Tracing



Transaction sample

Timestamp
10 hours ago (January 29th 2019, 21:59:45.991)

URL
N/A

Duration
32 ms

% of trace
100.00%

Result
N/A

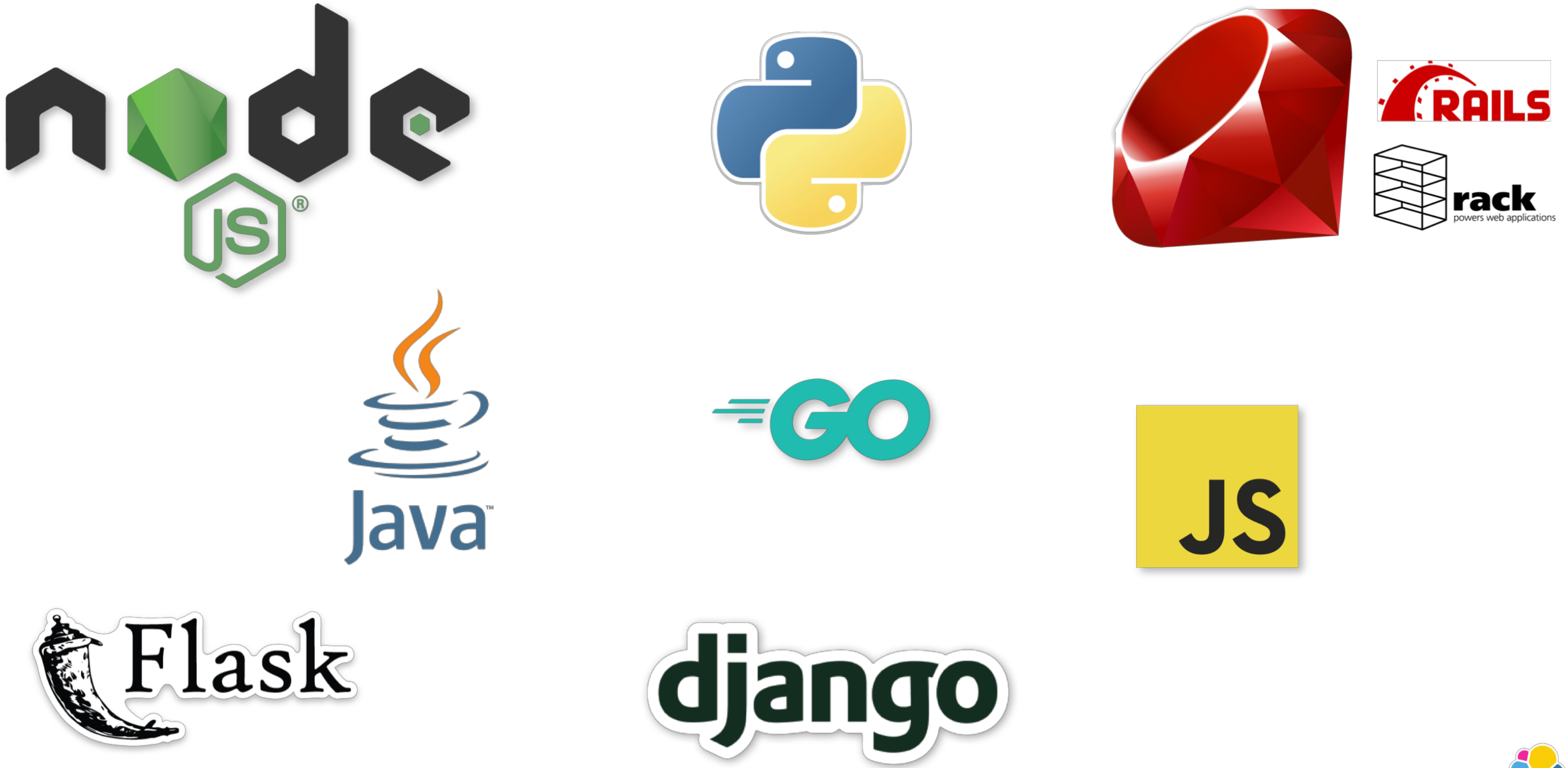
User ID
N/A

- Instrumented Services, interleaved
- See how services interact
- See External calls with details

Mix APM with other data & features

- APM data is **just another Elasticsearch index**
- Customize dashboards with other visuals to show what YOU want
- Mix with other Elastic Stack features, such as machine learning, alerting...
- Built-in integration with ML & Alerting

Supported Languages & Frameworks



elastic

Demo Time

Threat Hunting with Elastic

APM as part of Route Cause Analysis