



RED HAT
OPEN SOURCE DAY

Europe, Middle East & Africa



Elastic Stack: la soluzione per avere i dati sempre a portata di mano

STEFANO PAMPALONI
AMM. SEACOM SRL



#redhatosd



Chi è Seacom



Distributore italiano

Authorized Zimbra Training Center

Aggregator (mercato ISP)

Fondatore di...



RETE ITALIANA
OPEN SOURCE

Gli altri prodotti



from the creators of Kafka



Workflow Simplified



Seacom Premium partner Elastic



elastic



Elastic Overview



Statistics since 2012, start of the company



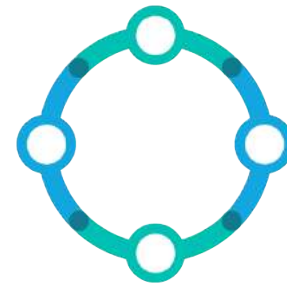
100,000+

Community
Members



130M+

Product
Downloads



3,700+

Subscription
Customers



Solving Problems Beyond 'Search'



“Migliora la cura dei pazienti aiutando a prendere le decisioni in tempo reale.”

“Aiuta a combattere il traffico di esseri umani.”

“Analisi di 3-4 miliardi di eventi al giorno per la security intelligence.”

“Trovare la camera giusta non è mai semplice (senza Elastic).”

“Molti ambiti di utilizzo: ottimizzazione del trading, analisi dei log, reclutamento del personale.”





High scale, not easily real-time, and high TCO



Key/value stores, schemaless, lack of analytical capabilities



Structured data, complex joins, not unstructured data



Custom & Proprietary Systems

Single use case, not built to support multiple use cases

Great tools exist but do they solve today's data problems in a way that is real-time, scalable, and relevant to drive revenue growth and reduce costs?

Today's Developer Requirements



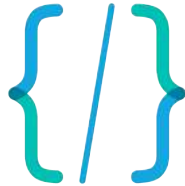
**Horizontal
Scale**



**Real-Time Data
Availability**



**Flexible Data
Model**



**Rapid Query
Execution**



**Sophisticated Query
Language**



Schemaless



Elastic Stack



X-Pack



Elastic Cloud

Application Search

Metrics Analytics

Log Analytics

Business Analytics

Security Analytics

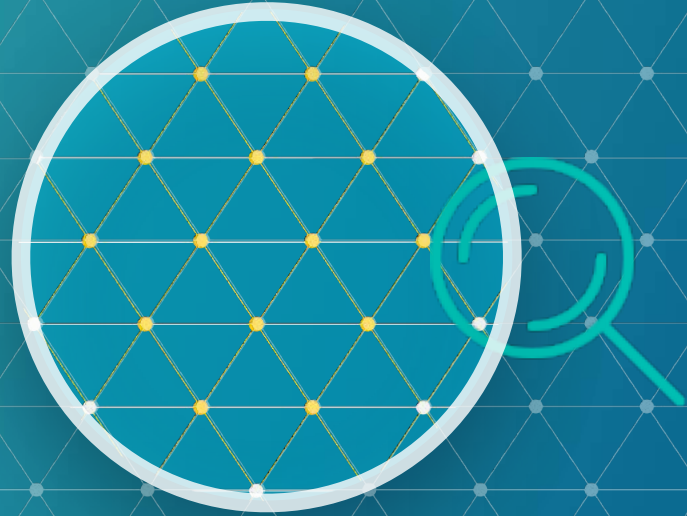
Many more ...

IoT

Recommendation

Search and analytics, it all started here

More than 60% of our customers have a search or analytics use case





➤ Marktplaats Alle groepen... Postcode Alle afstanden... Zoek

- Doe-het-zelf en Verbouw
- Fietsen en Brommers
- Hobby en Vrije tijd
- Huis en Inrichting
- Huizen en Kamers
- Kinderen en Baby's
- Kleding | Dames
- Kleding | Heren
- Klussen
- Motoren
- Muziek en Instrumenten
- Postzegels en Munten
- Sieraden en Tassen
- Spelcomputers, Games
- Sport en Fitness
- Telecommunicatie
- Tickets en Kaartjes
- Tuin en Terras
- Vacatures
- Vakantie
- Verzamelen

Nieuw en populair

<p>HEMA Poppenwagen G... € 20,00 Topadvertentie</p>	<p>Smoby Quinny poppen... € 38,95 Topadvertentie</p>	<p>Quinny poppenwagen v... € 39,95 Topadvertentie</p>	<p>Poppenwagen Smoby ... € 39,99 Topadvertentie</p>
---	--	---	---

Huis en Inrichting

<p>Vrijstaande rechthoeki... € 40,99 Topadvertentie</p>	<p>Barokspiegel (s) Zwart ... € 99,00 Topadvertentie</p>	<p>Kast met glas in lood € 250,00 Zoiest geplaatst: Vandaag 15:49</p>	<p>Bijzettafel set Cube € 69,95 Homepagina Advertentie</p>
---	--	---	--



Groupon

Home Local Goods Getaways Clearance Coupons Groupon-a-Thon

GROUPON-A-THON UP TO 80% OFF OVER 50,000 INCREDIBLE DEALS ONLY THRU FRIDAY Day 2! Save on Select Restaurants • Bars • Things to Do • More

results for "Yoga"

Sort by **Relevance**

Arlington Heights Des Plaines Evanston
View On Map
Jenners Grove SOUTH AVE
Map data ©2016 Google

- Local**
- Health & Fitness (675)
 - Things To Do (160)
 - Personal Services (17)
 - Beauty & Spas (11)
 - Retail (5)
- Goods**
- Sports & Outdoors (753)
 - Women's Fashion (93)
 - Electronics (73)
 - Entertainment (38)
 - Jewelry & Watches (18)
 - Baby, Kids & Toys (1)
 - Men's Fashion (0)
 - Health & Beauty (2)
 - For the Home (1)

ALMOST GONE

McPetridge Sports Center
Up to 52% Off Yoga Classes
Heated and unheated yoga classes such as Vinyasa Flow, Forrest, Sculpt, Restorative and Hatha
Chicago • 7.4 mi
~~\$100~~ **\$49**

Up to 83% Off Yoga at Chicago Oneness Center
Chicago Oneness Center
Buena Park • 7.2 mi
~~\$100~~ **\$29**

Up to 76% Off Yoga Classes
Cindy Huston
Buena Park • 7.2 mi
~~\$100~~ **\$29**



Assistenza Veloce
02 89.12.43.61

Contatti
Uso del Sito
Condizioni di Vendita

14 Anni
UfficioDiscount
la leggerezza dei prezzi

Accedi/Registrati
Area Personale

Lista preferiti

Categorie

Ricerca
Cartucce & Toner

cartella

CERCA

0 Carrello € 0

Home » Ricerca Prodotti



FILTRI

REPARTO

- Cartelle con elastico in PPL e PVC 37
- Cartelle porta disegni 8
- Cartelle a soffietto 9
- Cartelle con elastico in cartoncino 72
- Cartelle sospese per cassetto 52
- Classificatori 8
- Portablocchi per meeting 5
- Cartelline in 200

Trovati **848** prodotti cercando: **cartella**



Cartella personalizzabile
KreaCover® Exacompta -
59589E...[Leggi Tutto](#) »
• **Reparto:** Cartelle con elastico
in PPL e PVC
Cod. Prod. 407276

4,05 € IVA escl. 4,94€ IVA incl.
(4,05 € al pz. venduto in confezioni da 1 pz.)

1

Aggiungi

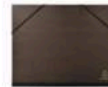
Più acquisti, meno spendi

€ 3,89 Acquisto conf. da 6 a 11
€ 3,85 Acquisto conf. oltre 11



[Aggiungi ai preferiti](#)

0 Disponibili Info



Cartelle porta disegni
Exacompta - 50x65 cm -
548800E...[Leggi Tutto](#) »
• **Reparto:** Cartelle porta
disegni
Cod. Prod. 129909

9,98 € IVA escl. 12,18€ IVA incl.
(9,98 € al pz. venduto in confezioni da 1 pz.)

1

Aggiungi

Più acquisti, meno spendi

€ 9,73 Acquisto conf. da 5 a 9
€ 9,66 Acquisto conf. oltre 9



[Aggiungi ai](#)

19 Disponibili Info

Opinioni dei clienti

feedaty
Opinioni Certificate



RECENSIONI TOTALI

23.638

ULTIMI 12 MESI

3.623

★★★★★

Serve **AIUTO?**

Chiedi a noi



Prodotti correlati



Copriquaderno Maxi
in PP Favorit - 21x30
€ 0,70



Maxi Pennello Giotto
- setola - 536100
€ 1,28



Carta Crespa CWR -
50x250 cm - bianco -
€ 0,58



Carta Crespa CWR -
50x250 cm - giallo -
€ 0,58



Carta Crespa CWR -
50x250 cm - arancio -
€ 0,58

Altri utenti hanno comprato anche



Punti universali
Zenith - Punti
€ 0,75



Carta 5 star Bianca -
A4 - 80 g - 961303
€ 12,50



Marcatore
permanente Pentel -
€ 0,82



Asciugamani premio
C Lucart - 1 velo -
€ 1,18



Punti universali Rapid
- Punti metallici 21/4
€ 0,42

Logs Logs Logs, many devices, many systems

More than 40% of our
customers use our
products
for operational log
analysis



verizon^v

We collect more than
1.2 TB logs every day from
our infrastructure, web
servers, and applications.



We handle more than
3 billion daily events while
meeting all of our data security
requirements.



Equitalia

Log applicativi e di sistema

Provvedimento Garante Privacy
accessi Amm. Sistemi

Sniff sniff sniff, find the bad actors in your data

200% YoY growth in
security use cases with
our products





We mine and analyze
4 billion events every day to
detect security hacks and threats.



We analyze piles of data:
13B AMP queries/day
600B emails/day
16B web requests/day



Telco Italiana

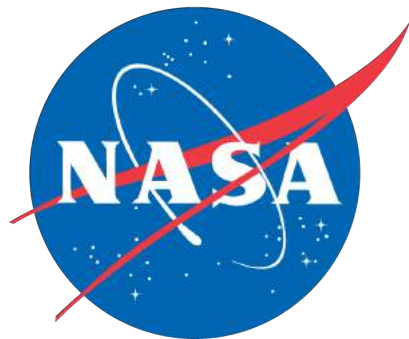
150TB totali
600Gb/day
Intrusion detection
Comportamenti anomali

**75% of our customers
use our products for
multiple use cases**





1,000+ developers use the Elastic Stack for use cases from trade tracking to creating new HR and compliance apps.



We send from Mars more than
30K messages
100K documents
4x a day for
operational, telemetry, anomaly
resolution, and log analysis.



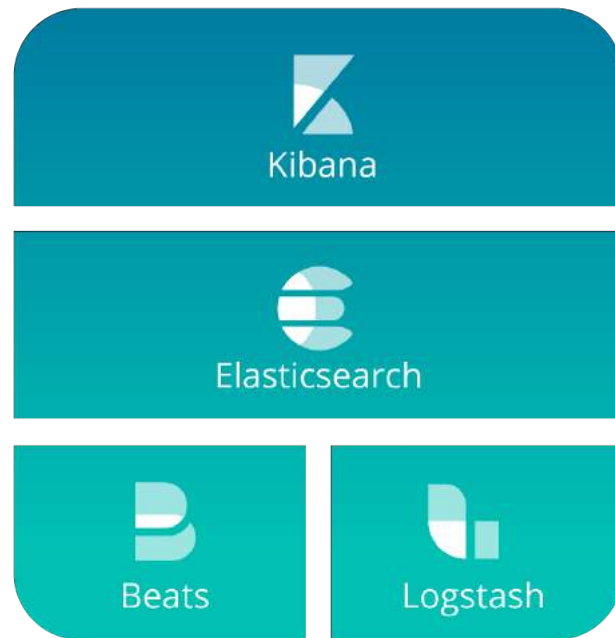
Accenture

Piattaforma di content delivery
per Broadcasting



Elastic Stack

100% open source
No enterprise edition
All new versions with 5.0





X-Pack

Single install
Extensions for the Elastic Stack
Subscription pricing



Security



Alerting



Monitoring



Reporting



Graph

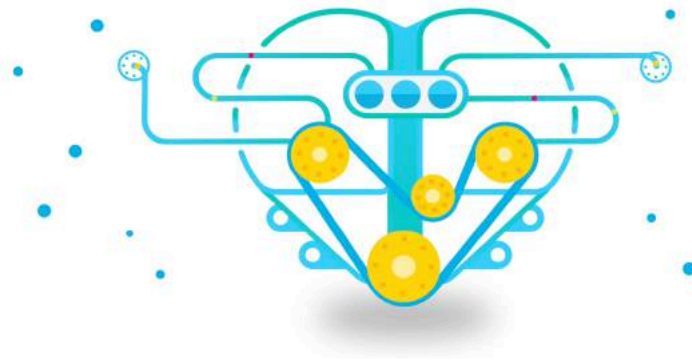


Machine Learning



Elasticsearch

Heart of the Elastic Stack



Distributed, Scalable

High-availability

Multi-tenancy

Developer Friendly

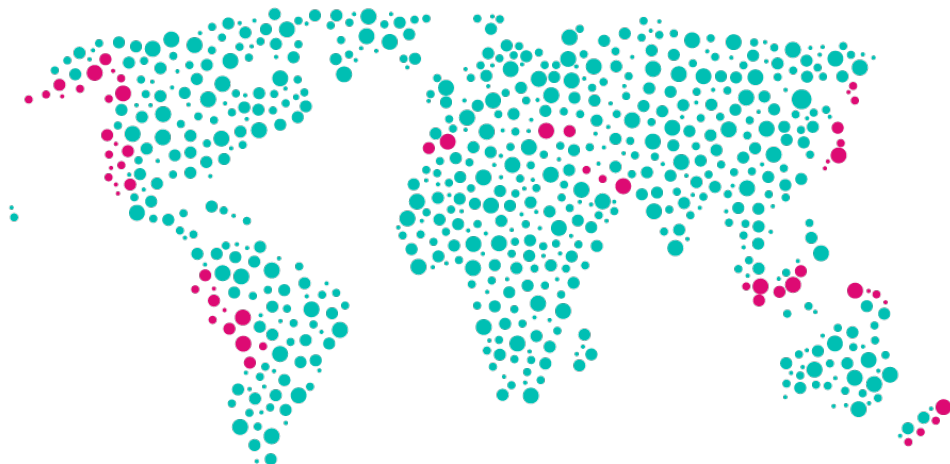
Real-time, Full-text Search

Aggregations



Kibana

Window into the Elastic Stack



Visualize and analyze

Graph Exploration

Geospatial

UX to secure and manage
the Elastic Stack

Customize and Share
Reports

Build Custom Apps



- Discover
- Visualize
- Dashboard
- Graph
- Monitoring
- Timeline
- Management
- Dev Tools

Total Visitors

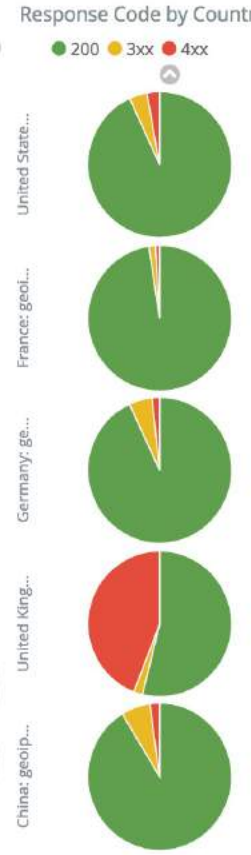
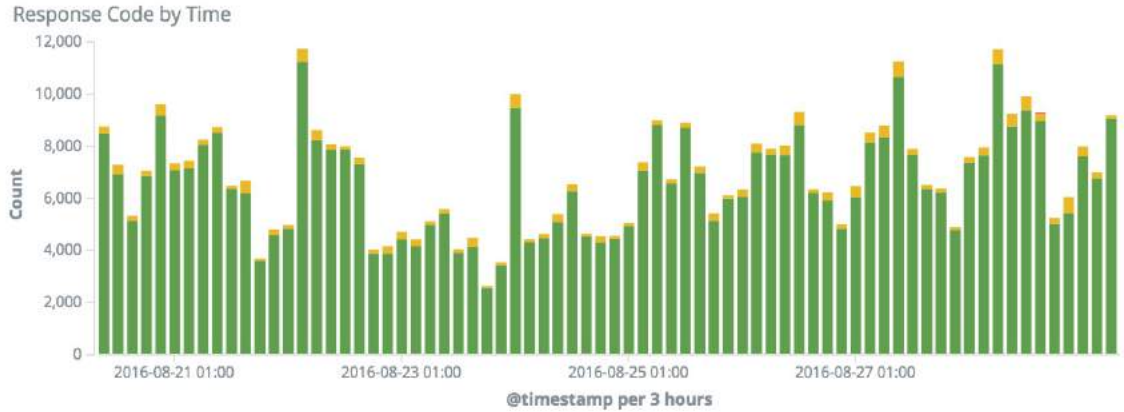
541,194

Total IPs

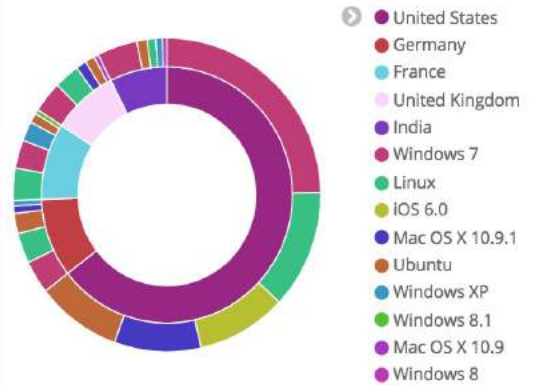
Unique Visitors

10,279

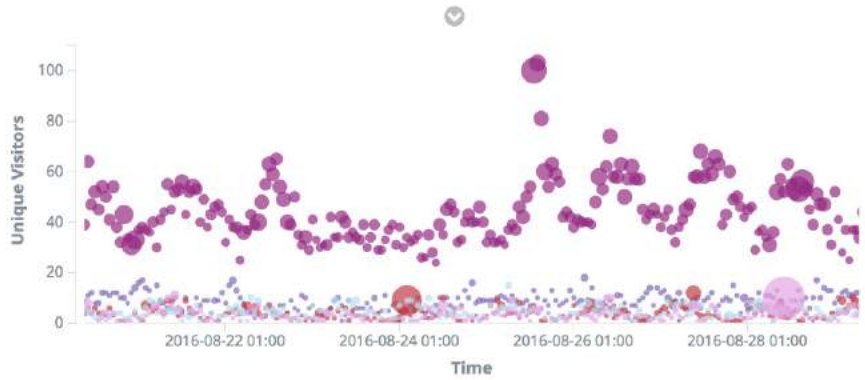
Unique IPs



Traffic by Country & OS



Bytes vs. Time



Unique Visits by City

City	Unique Visitors	Total Visitors
Beijing	346	8,232

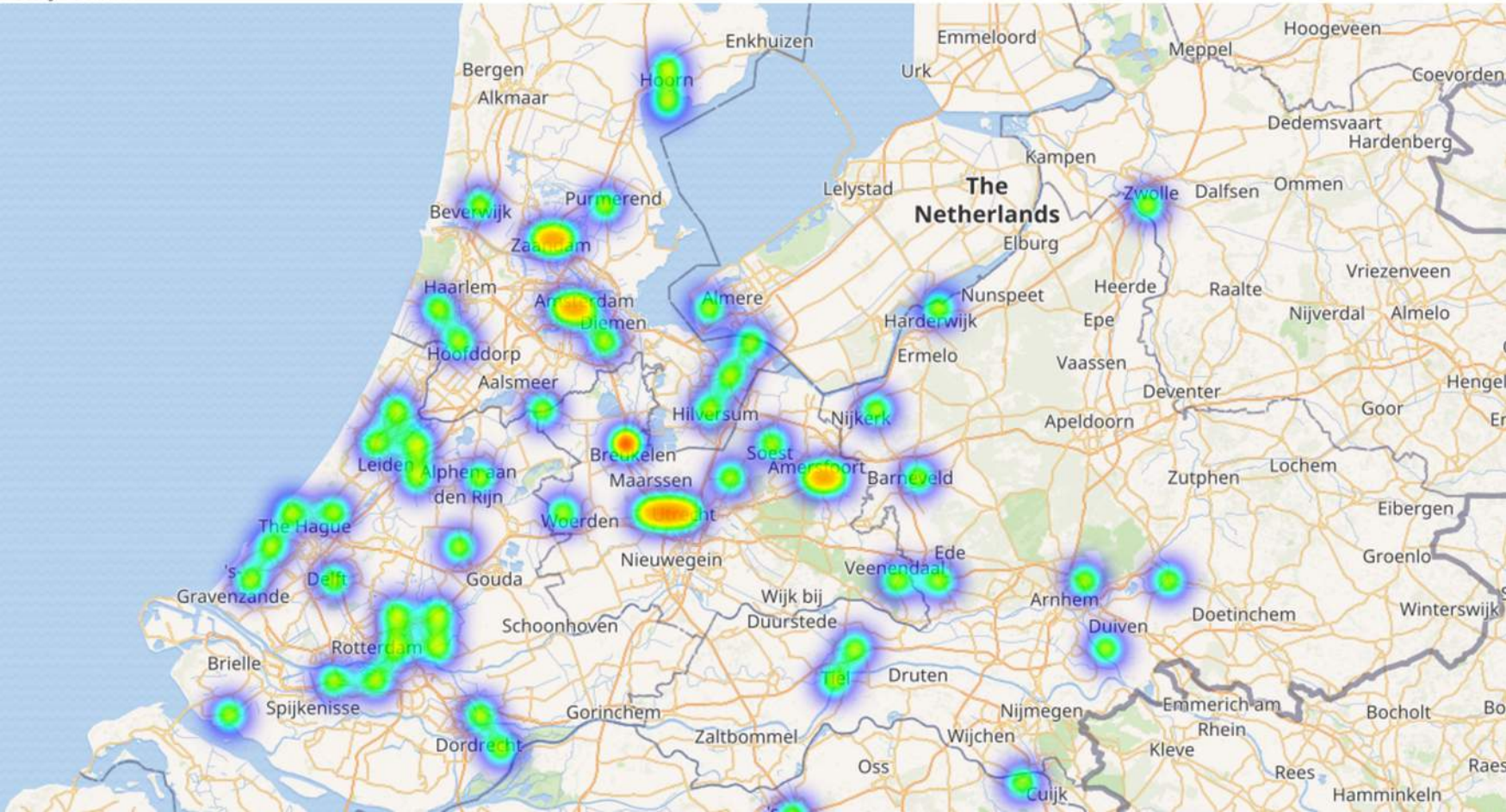
Traffic vs. Location



*



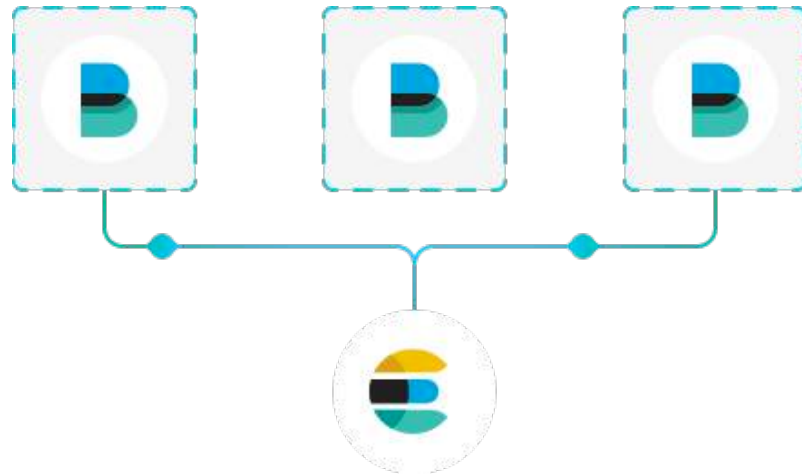
Web Traffic by Location





Beats

Window into the Elastic Stack



Ship data from the source	Ship and centralize in Elasticsearch	Ship to Logstash for transformation and parsing
Ship to Elastic Cloud	Libbeat: API framework to build custom beats	30+ community Beats



FILEBEAT
Log Files



METRICBEAT
Metrics



PACKETBEAT
Network Data



WINGLOGBEAT
Window Events

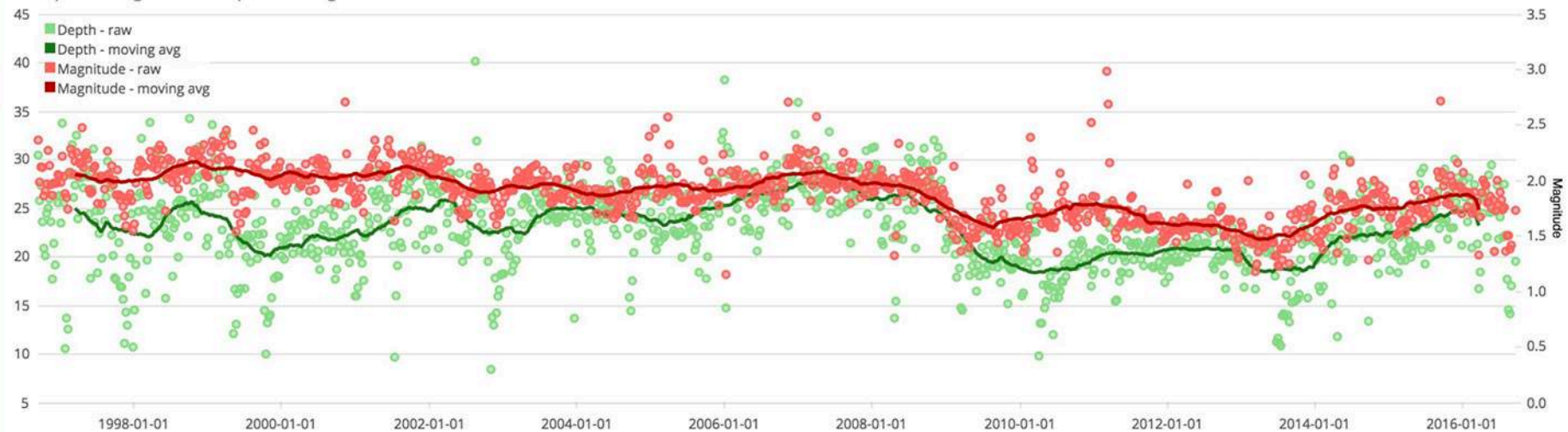
More than 30 community Beats
and growing ...

Apachebeat, dockbeat, httpbeat,
mysqlbeat, nginxbeat, redis beats,
twitterbeat, and more

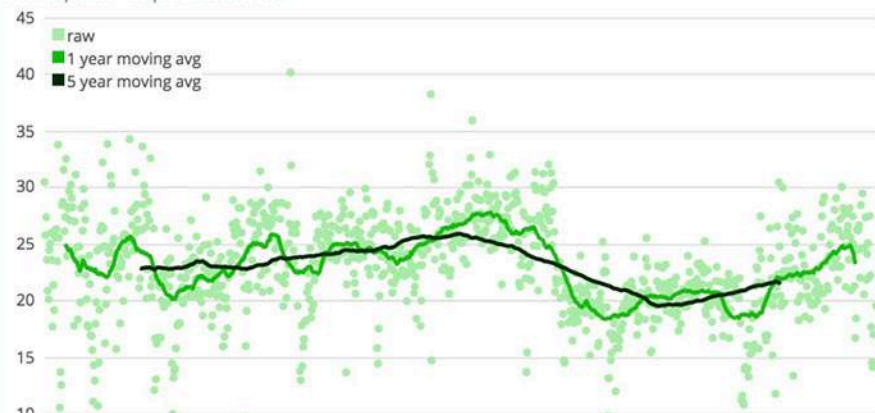
*



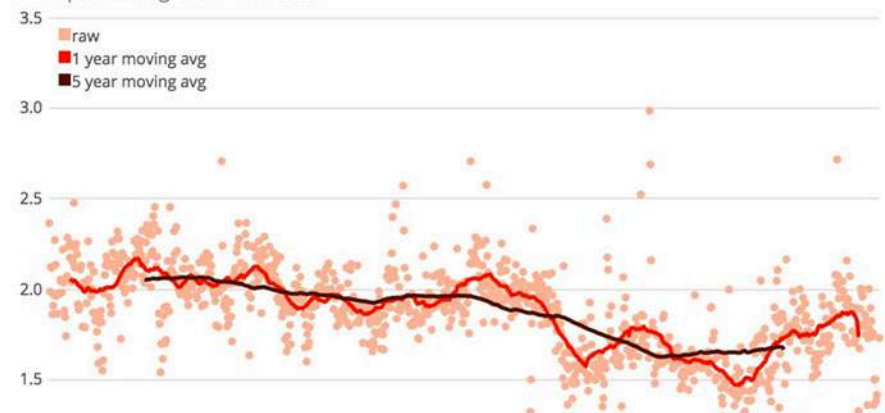
Earthquake - Magnitude vs Depth Mov. Avg



Earthquake - Depth Timeseries



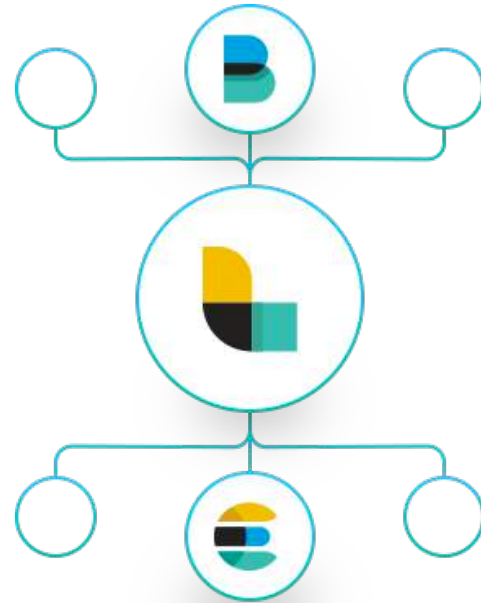
Earthquake - Magnitude Timeseries





Logstash

Data processing pipeline



Ingest data of all shapes, sizes, and sources

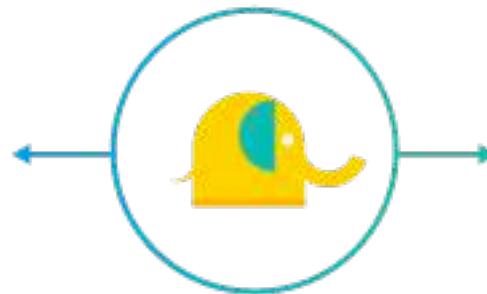
Parse and dynamically transform data

Transport data to any output

Secure and encrypt data inputs

Build your own pipeline

More than 200+ plugins



ES-Hadoop

Elasticsearch for Hadoop

Two-way connector

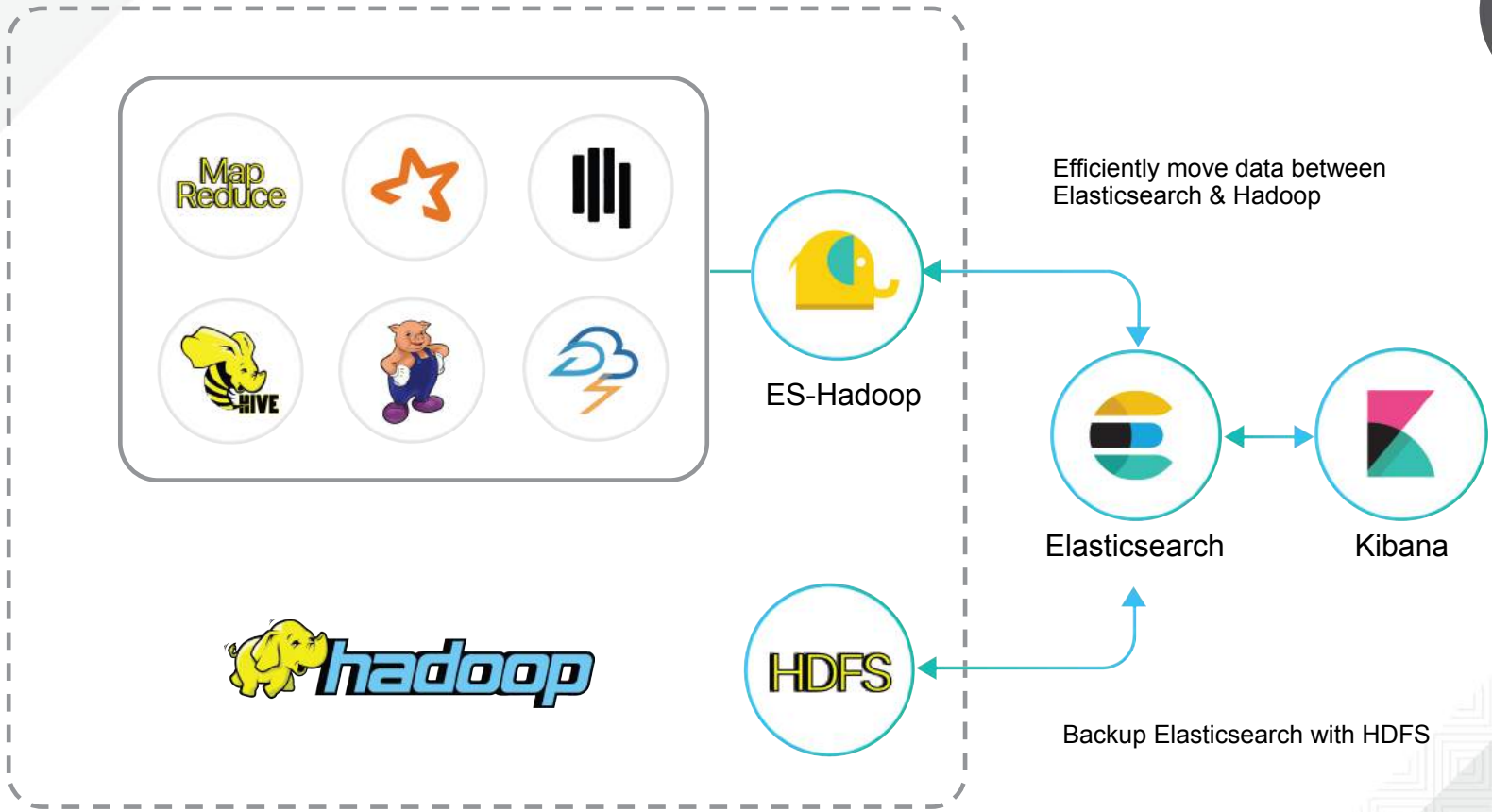
Index Hadoop data in
Elasticsearch

Enable real-time search
capabilities

Visualize HDFS data
in Kibana

Snapshot and restore
with HDFS

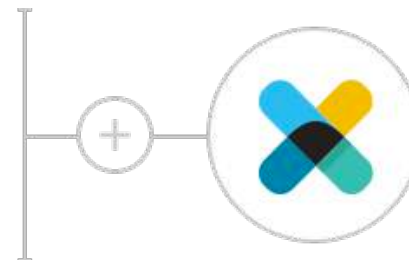
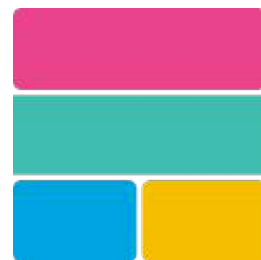
Support for Spark, Storm
MapReduce, and more





X-Pack

Extensions for the Elastic Stack



Security

Alerting

Monitoring

Reporting

Graph Analytics

Single Install, included in
Elastic Subscription



X-Pack

Security

AUTHENTICATION

- Username and password
- Integrate with authentication systems
- Create a custom realm to authenticate users

AUTHORITIZATION

- Manage users and roles
- Assign permissions and privileges

ADDITIONAL CONTROLS

- SSL/TLS encryption
- IP filtering
- Field and document level security
- Audit logging

- Discover
- Visualize
- Dashboard
- Graph
- Monitoring
- Timelion
- Management
- Dev Tools

Edit Role

[Return to All Roles](#) [Delete](#) [Save](#)**Name**

Cluster Privileges

 all monitor manage manage_security manage_index_templates

Run As Privileges

Indices Privileges

- all
- manage
- monitor
- index
- create
- delete
- write
- delete_index



- elastic
- Logout
- Collapse



X-Pack

Alerting

SETUP ALERTS

- Create Watches to detect changes in your data
- Trigger automatic notifications
- Setup nested alerts
- Store and track alert history

NOTIFY AND INTEGRATE

- Email
- Slack
- Pagerduty
- Hipchat or JIRA
- Other monitoring systems

kibana

- Discover
- Visualize
- Dashboard**
- Monitoring
- Timelion
- Management
- Dev Tools

- elastic
- Logout
- Collapse

* 🔍

Alert Conditions Evaluated

173

of alerts evaluated

Alerts Triggered

22

of alerts fired

Alerts Throttled

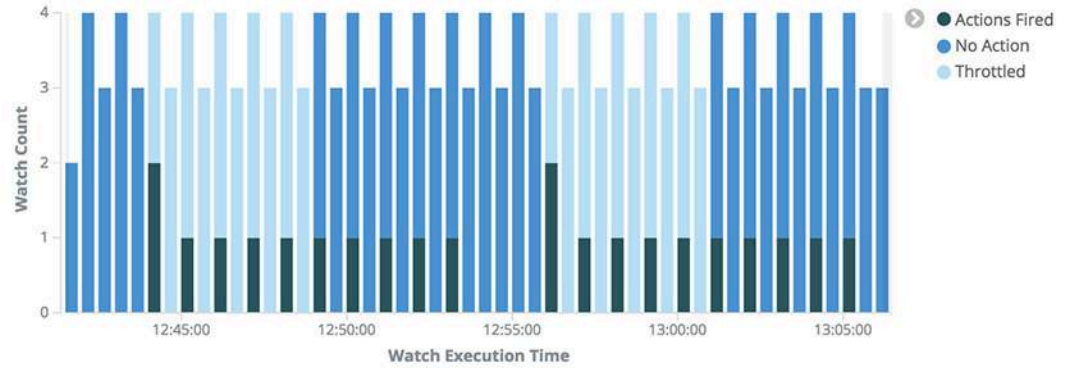
58

of alerts fired

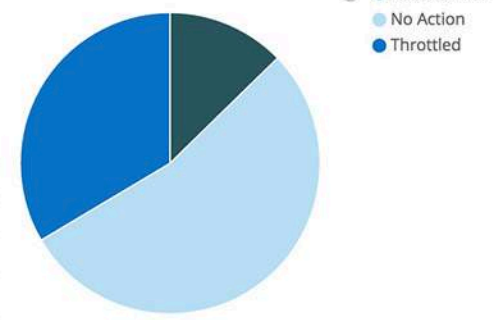
Most Frequent Watches with Met Condition

watch_id: Descending ↕ Q	Count ↕
dir-traversal	60
port-scan	20

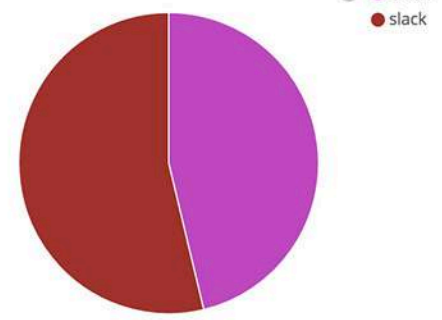
Alert Status over Time



Actions



Execution Status





X-Pack

Monitoring

MONITOR CLUSTER HEALTH

- Prebuilt Kibana dashboards to monitor the performance of the Elastic Stack
- Get vital statistics at various levels -- cluster, node, and indices

OPTIMIZE CLUSTER PERFORMANCE

- Multicluster support to compare health and performance of multiple clusters
- Analyze historical or real-time data for root cause analyses
- Utilize analyses to proactively optimize and improve cluster performance
- Configure data retention policy

- Discover
- Visualize
- Dashboard
- Graph
- Monitoring**
- Timelion
- Management
- Dev Tools

3 of 3

Name ↓	Status	Nodes	Indices	Data	Kibana	License
prod01		24	192	73.1 GB	1	Platinum Expires 1 Feb 17
Monitor *		2	8	218.5 MB	1	Platinum Expires 1 Feb 17
dev-test		19	233	181.5 GB	1	Trial Expires 10 Nov 16

- elastic
- Logout
- Collapse

✓ Nodes: **3**
 Indices: **3**
 Memory: **2GB / 6GB**
 Total Shards: **22**
 Unassigned Shards: **0**
 Documents: **174,544,212**
 Data: **101GB**
 Uptime: **118 hours**
 Version: **5.0.0-beta1**

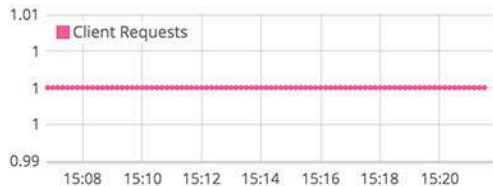
Nodes 3 of 3

Name	Status	CPU Usage	JVM Memory	Load Average	Disk Free Space	Shards
★ prod-1 <small>127.0.0.1:9300</small>	✓	0% ↓ <small>2% max 1% min</small>	40% ↑ <small>43% max 16% min</small>	2.82 ↓ <small>5.48 max 2.5 min</small>	309.6 GB ↓ <small>309.7 GB max 309.5 GB min</small>	7
☰ prod-2 <small>127.0.0.1:9301</small>	✓	2% ↓ <small>2% max 1% min</small>	16% ↓ <small>42% max 16% min</small>	2.82 ↓ <small>5.48 max 2.5 min</small>	309.6 GB ↓ <small>309.7 GB max 309.5 GB min</small>	8
☰ prod-3 <small>127.0.0.1:9302</small>	✓	1% ↓ <small>3% max 1% min</small>	32% ↓ <small>43% max 17% min</small>	2.82 ↓ <small>5.28 max 2.38 min</small>	309.6 GB ↓ <small>309.7 GB max 309.5 GB min</small>	7

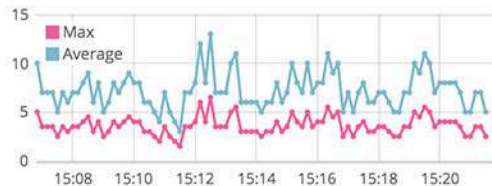
localhost:5552 OS Free Memory: 696.8 MB Version: 5.0.0-beta1

- Discover
- Visualize
- Dashboard
- Graph
- Monitoring
- Timelion
- Management
- Dev Tools

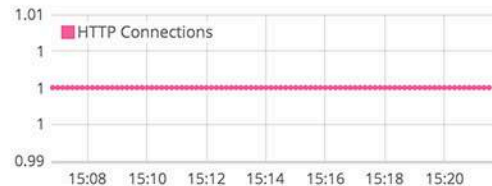
Client Requests



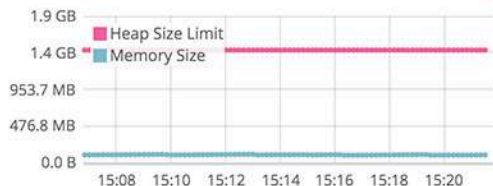
Client Response Time (ms)



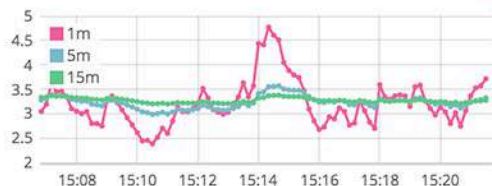
HTTP Connections



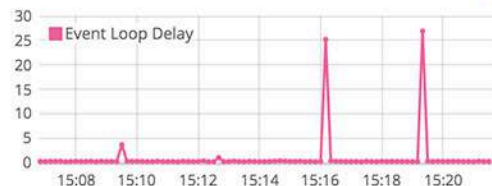
Memory Size (GB)



System Load



Event Loop Delay (ms)





X-Pack

Reporting

AUTOMATE SCHEDULING








- Email recurring status updates daily, weekly, monthly, etc.
- Combine reporting with X-Pack alerting capabilities to trigger conditional reports

SHARE AND COLLABORATE

- Export any Kibana visualization or dashboard
- Print-optimized and PDF formatted
- Download and share past reports

Generated Reports

 Filter Reports: Only show my reports

Document	Added	Status	Actions
Metrics Dashboard dashboard	2016-09-30 @ 10:02 AM elastic	processing 2016-09-30 @ 10:02 AM	
Web Traffic by Location visualization	2016-09-30 @ 10:01 AM elastic	completed 2016-09-30 @ 10:01 AM	
Traffic by Country & Device visualization	2016-09-30 @ 10:00 AM elastic	completed 2016-09-30 @ 10:01 AM	
Dashboard Overview visualization	2016-09-30 @ 10:00 AM elastic	completed 2016-09-30 @ 10:01 AM	
Web Analytics dashboard	2016-09-30 @ 9:59 AM elastic	completed 2016-09-30 @ 9:59 AM	
Alert History dashboard	2016-09-30 @ 9:57 AM elastic	completed 2016-09-30 @ 9:57 AM	
Metrics Dashboard dashboard	2016-09-23 @ 2:39 PM elastic	completed 2016-09-23 @ 2:39 PM	
Metrics Dashboard dashboard	2016-09-20 @ 7:44 PM elastic	completed 2016-09-20 @ 7:45 PM	



X-Pack

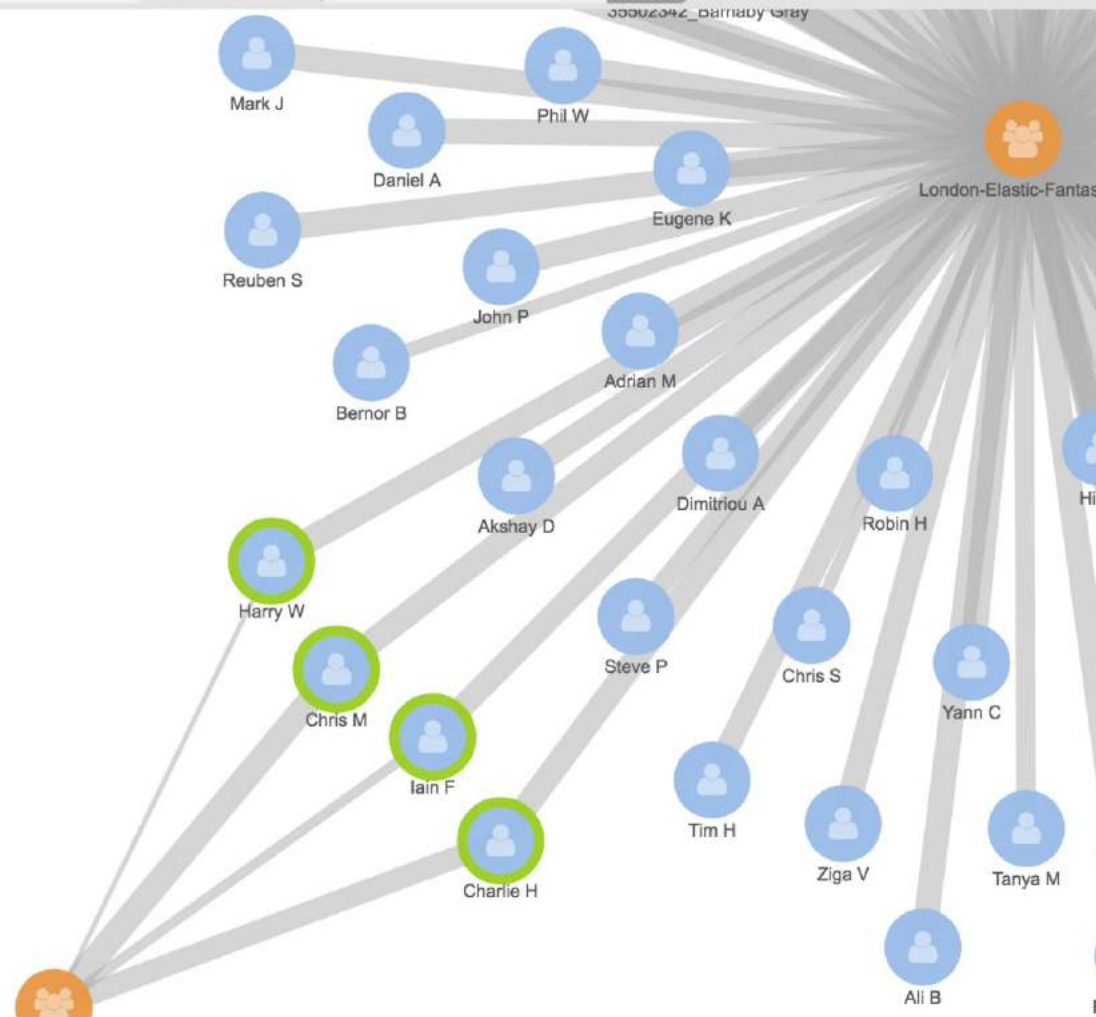
Graph

A NEW WAY TO EXPLORE DATA

- Uses relevance capabilities of Elasticsearch
- Discover linkages and connections
- Leverage API and UI-drive tool

EXTEND TO NEW USE CASES

- Fraud discovery
- Recommendations
- Cyber security
- Behavioral analyses



Toolbar icons: undo, redo, add, link, delete, zoom, edit, info, play

Selections

all none invert linked

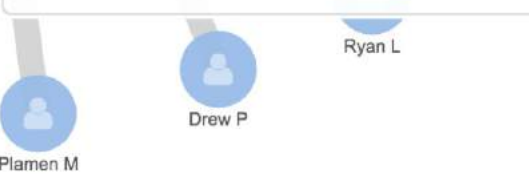
- Charlie H
- Iain F
- Chris M
- Harry W

Graph visualization icons: bar chart, refresh

member_id 13469970_Harry Wayne

group

Display label Harry W
Change the label for this vertex





X-Pack

Machine Learning

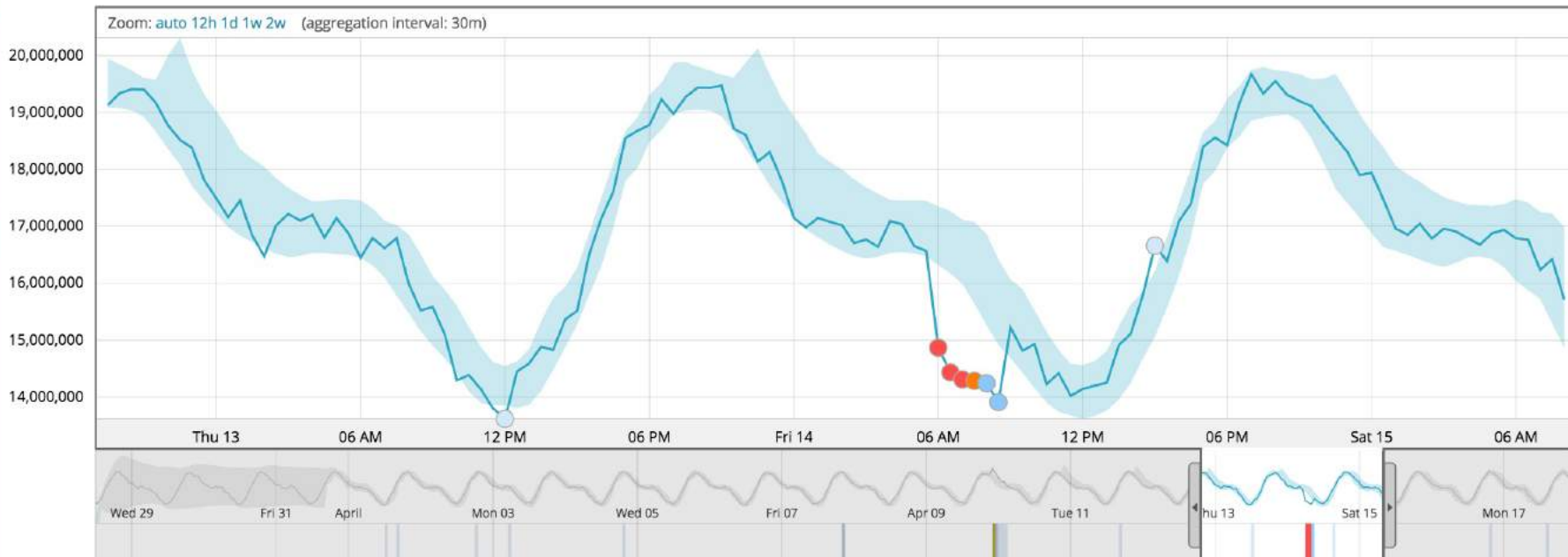
UNSUPERVISED MACHINE LEARNING

- Automatically detect anomalies
- Advanced correlation and categorization
- Identify root cause(s)
- Expose early warning signs

ENABLE NEW USE CASES

- Analyze time series data
- Expand security, IT Ops, fraud, finance, and many more use cases
- Available as beta in the 5.4 release

Time series analysis



Anomalies

Severity threshold: ▲ warning ▾

Interval: Auto ▾

time ↕	max severity ↕	detector ↕	actual ↕	typical ↕	description ↕	job ID ↕
▶ April 14th 2017, 06:00	▲ 95	sum(total) (total-request)	14432600	16609200	↓ 1.2x lower	total-request
▶ April 14th 2017, 07:00	▲ 83	sum(total) (total-request)	14310100	16421500	↓ 1.1x lower	total-request
▶ April 14th 2017, 08:00	▲ 24	sum(total) (total-request)	13909700	15499400	↓ 1.1x lower	total-request
▶ April 13th 2017, 12:00	▲ 1	sum(total) (total-request)	13615600	14113400	↓ Unusually low	total-request
▶ April 14th 2017, 15:00	▲ < 1	sum(total) (total-request)	16659900	15863700	↑ 1.1x higher	total-request

Job settings

Fields

- event rate Count
- accept Mean
- deny Mean
- response Mean
- total Sum

Bucket span ⓘ

30m

Split Data

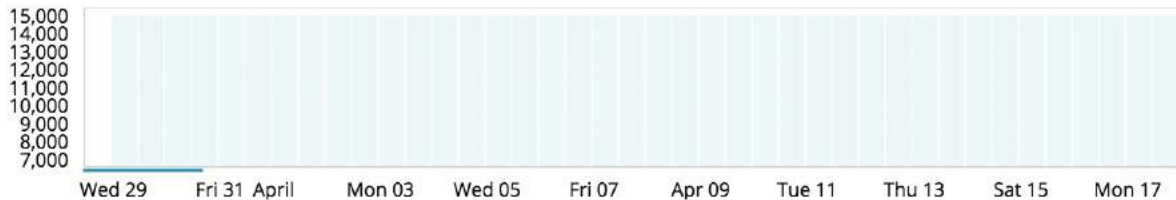
service.keyword

Key Fields

- host.keyword
- service.keyword

Results

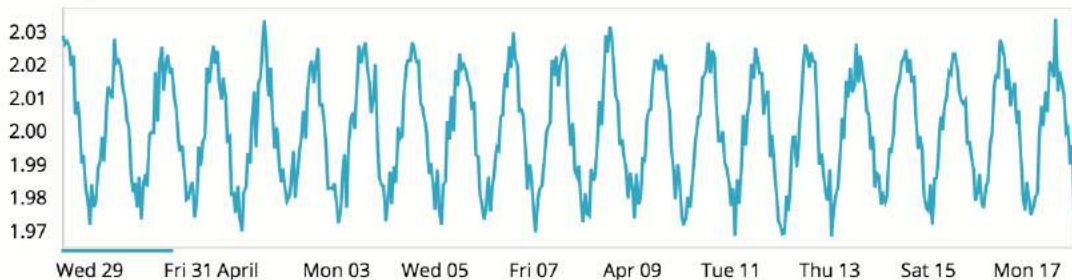
Document count



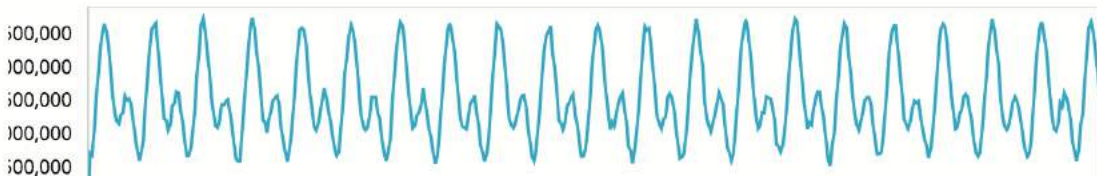
Data split by service.keyword



Mean response



Sum total



New job from index pattern server*

Chart interval: 1h [Use full server* data](#)

Aggregation ?

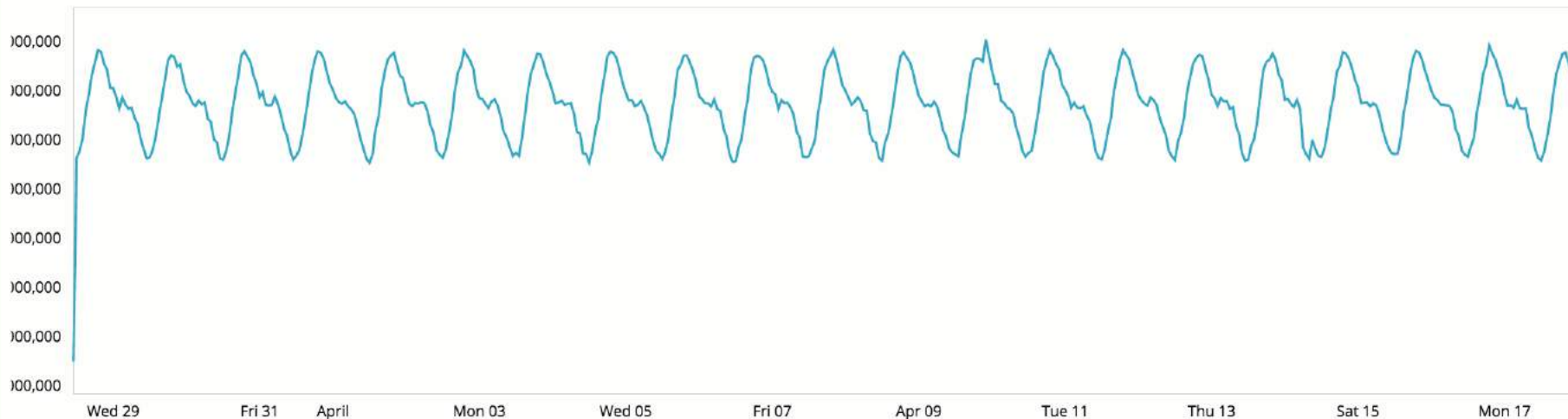
Sum

Field ?

total

Bucket span ?

60m



Name ?

total-requests

Description ?

job description

Advanced ?

Create Job



host.keyword

server_2

97

826

server_1

94

808

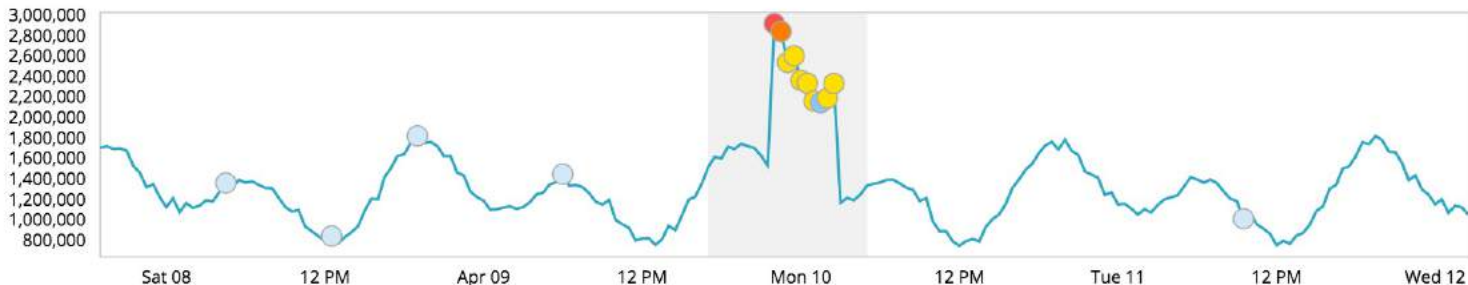
server_3

71

263

Anomalies

sum(total) (metric-by-appl) - service.keyword app_4 ⓘ



Severity threshold: ▲ major

Interval: Auto

time	max severity	detector	found for	influenced by	actual	typical	description	job ID
▼ April 9th 2017, 22:00	▲ 81	sum(total) (metric-by-appl)	app_4	host.keyword: server_2 host.keyword: server_1 service.keyword: app_4	2922690	1483330	▲ 2x higher	metric-by-appl

Description:

critical anomaly in sum(total) (metric-by-appl) found for service.keyword app_4

Details on highest severity anomaly:

service.keyword: app_4
time: April 9th 2017, 22:00:00 to April 9th 2017, 22:30:00
function: sum
fieldName: total
actual: 2922690
typical: 1483330
job ID: metric-by-appl
probability: 2.24588e-25

Influenced by:

host.keyword: server_2
host.keyword: server_1
service.keyword: app_4

Altro su Seacom & Elastic

Per ulteriori dettagli potete visitare le sezioni di Seacom dedicate a Elastic Stack

[Corsi Ufficiali](#)

[Use case](#)

[Video di presentazione](#)





RED HAT OPEN SOURCE DAY

Europe, Middle East & Africa



#redhatosd