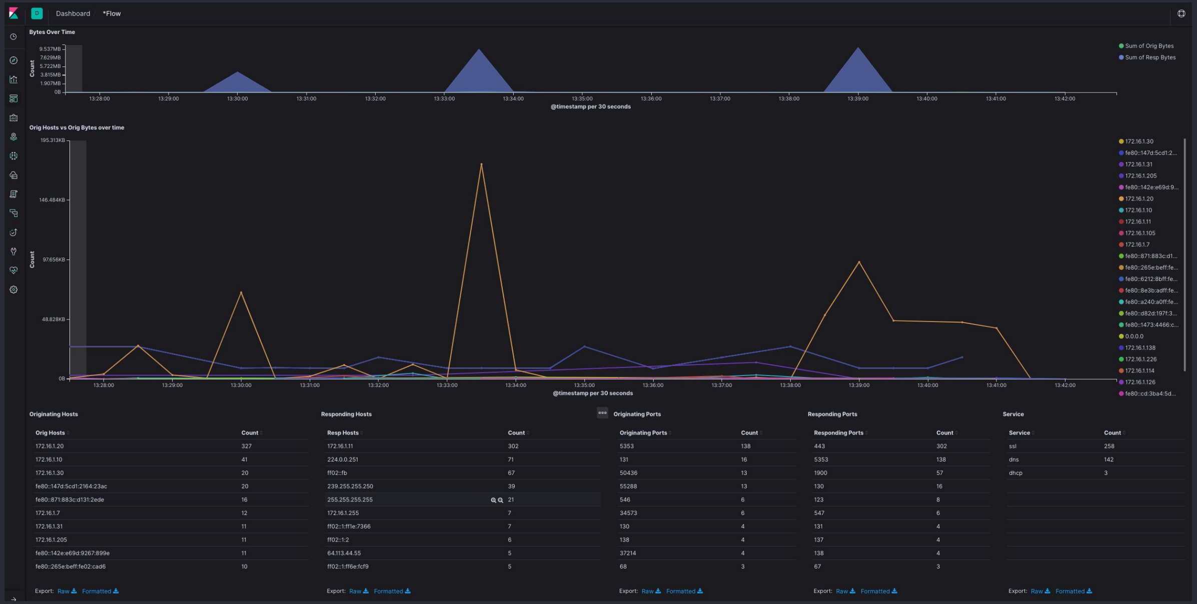
Kibana for Operators

Kibana for Operators Outline

- Introduction to Kibana
- Kibana Tabs
- Kibana Searching
- Building Kibana Visualizations
- Building Dashboards
- Alerting with Watcher
- Graphing
- Machine Learning

What is Kibana?

- Web UI for Elasticsearch
- Query and Filter
- Dashboards
- Live visualization



Originating Hosts

Orig Hosts	Count
172.16.1.20	327
172.16.1.10	41
172.16.1.30	20
fe80::147d:5cd1:2164:23ac	20
fe80::871:883c:d131:2ede	16
172.16.1.7	12
172.16.1.31	11
172.16.1.205	11
fe80::142e:e69d:9267:899e	11
fe80::265e:beff:fe02:cad6	10

Export: Raw Formatted

Responding Hosts

Resp Hosts	Count
172.16.1.11	302
224.0.0.251	71
ff02::fb	67
239.255.255.250	39
255.255.255.255	21
172.16.1.255	7
ff02::1:ff1e:7366	7
ff02::1:2	6
64.113.44.55	5
ff02::1:ff6e:fcf9	5

Export: Raw Formatted

Originating Ports

Originating Ports	Count
5353	138
131	16
50436	13
55288	13
546	6
34573	6
130	4
138	4
37214	4
68	3

Export: Raw Formatted

Responding Ports

Responding Ports	Count
443	302
5353	138
1900	57
130	16
123	8
547	6
131	4
137	4
138	4
67	3

Export: Raw Formatted

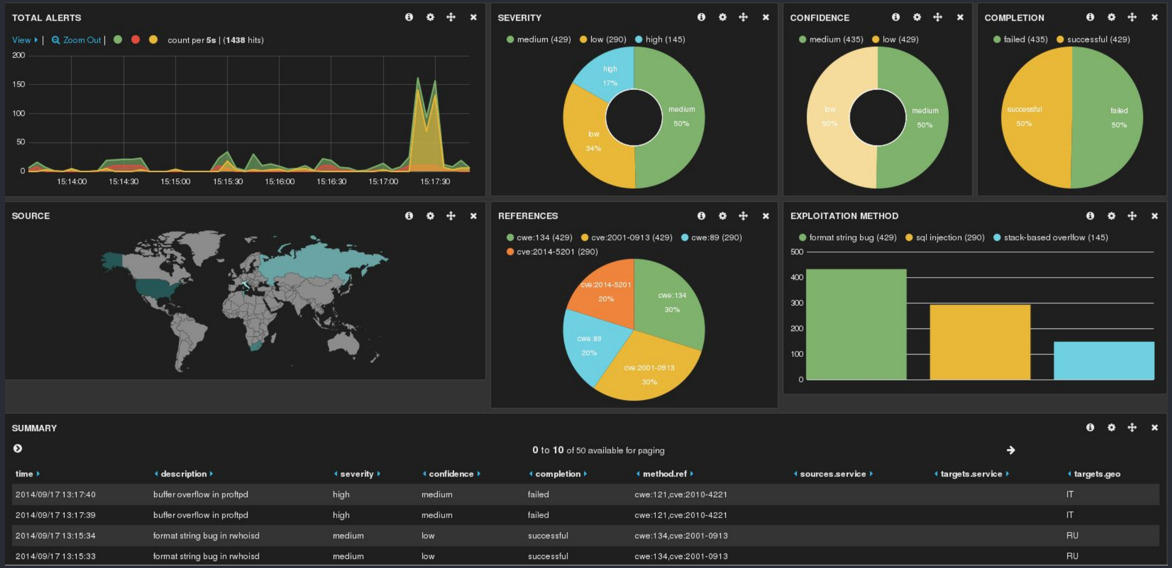
Service

Service	Count
ssl	258
dns	142
dhcp	3

Export: Raw Formatted

Data Visualization

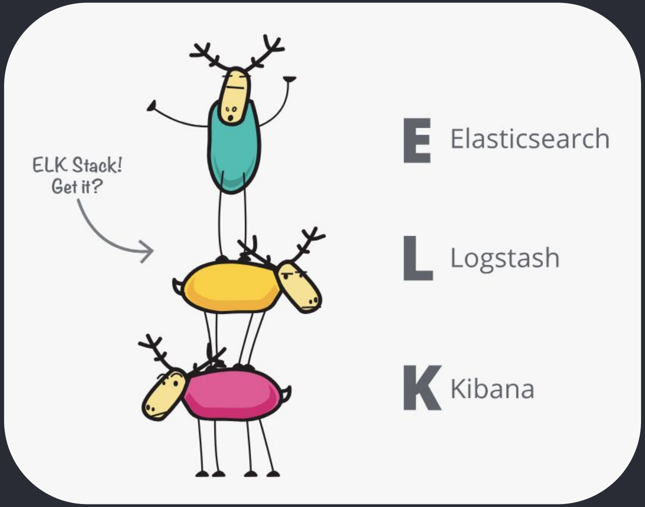
- Data as images
- Live updates
- Why visualize?

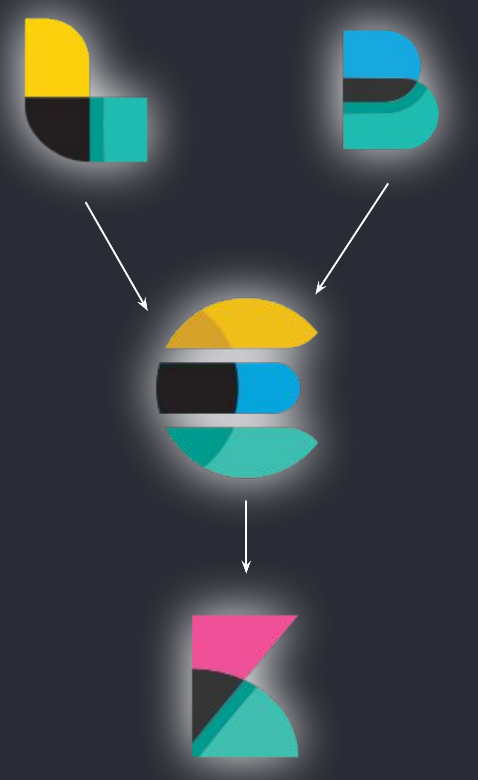

TOTAL ALERTS
View ▸ | Zoom Out | ● ● ● count per 5s | (1438 hits)
200
150
100
50
0
15:14:00
15:14:30
15:15:00
15:15:30
15:16:00
15:16:30
15:17:00
15:17:30
SEVERITY
● medium (429) ● low (290) ● high (145)
high 17%
medium 50%
low 34%
CONFIDENCE
● medium (435) ● low (429)
low 50%
medium 50%
COMPLETION
● failed (435) ● successful (429)
successful 50%
failed 50%
SOURCE
REFERENCES
● cwe:134 (429) ● cve:2001-0913 (429) ● cwe:89 (290) ● cve:2014-5201 (290)
cve:2014-5201 20%
cwe:134 30%
cwe:89 20%
cve:2001-0913 30%
EXPLOITATION METHOD
● format string bug (429) ● sql injection (290) ● stack-based overflow (145)
500
400
300
200
100
0
SUMMARY

0 to 10 of 50 available for paging

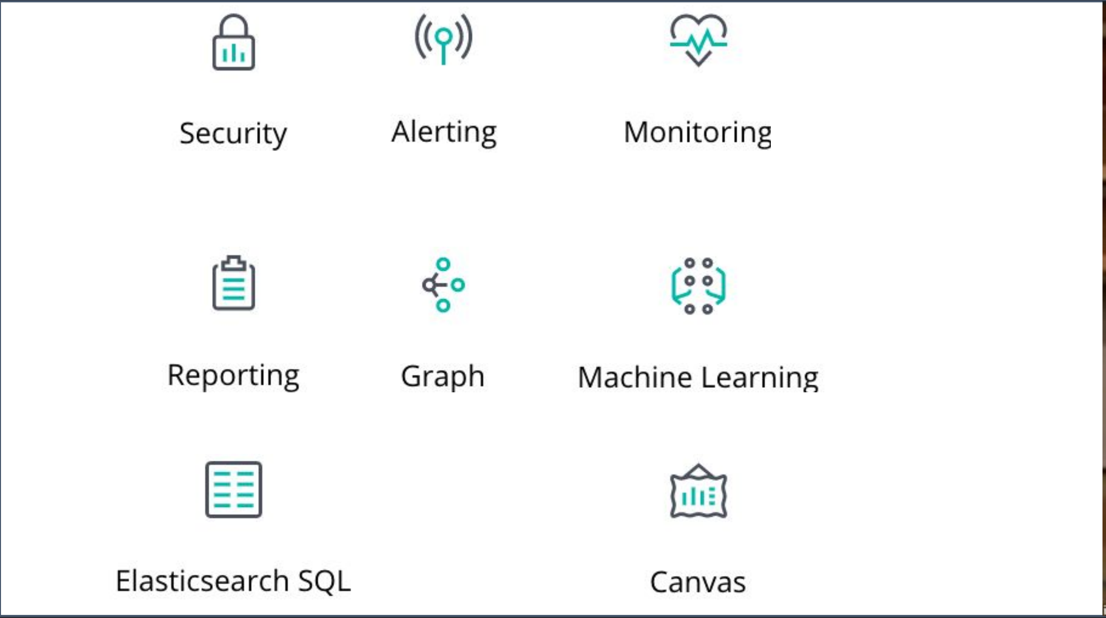
time	description	severity	confidence	completion	method.ref	sources.service	targets.service	targets.geo
2014/09/17 13:17:40	buffer overflow in proftpd	high	medium	failed	cwe:121,cve:2010-4221			IT
2014/09/17 13:17:39	buffer overflow in proftpd	high	medium	failed	cwe:121,cve:2010-4221			IT
2014/09/17 13:15:34	format string bug in rwhoisd	medium	low	successful	cwe:134,cve:2001-0913			RU
2014/09/17 13:15:33	format string bug in rwhoisd	medium	low	successful	cwe:134,cve:2001-0913			RU

Architecture





Licensed Features



Security

Alerting

Monitoring

Reporting

Graph

Machine Learning

Elasticsearch SQL

Canvas

YOU GET ENTERPRISE FEATURES!
EVERYONE GETS ENTERPRISE FEATURES!!
imgflip.com

License Management

Kibana Setup

- Open a web browser and go to http://classroom.perched.io:5601
- Make sure you have access to Kibana
- We will be creating our own spaces

Management Settings

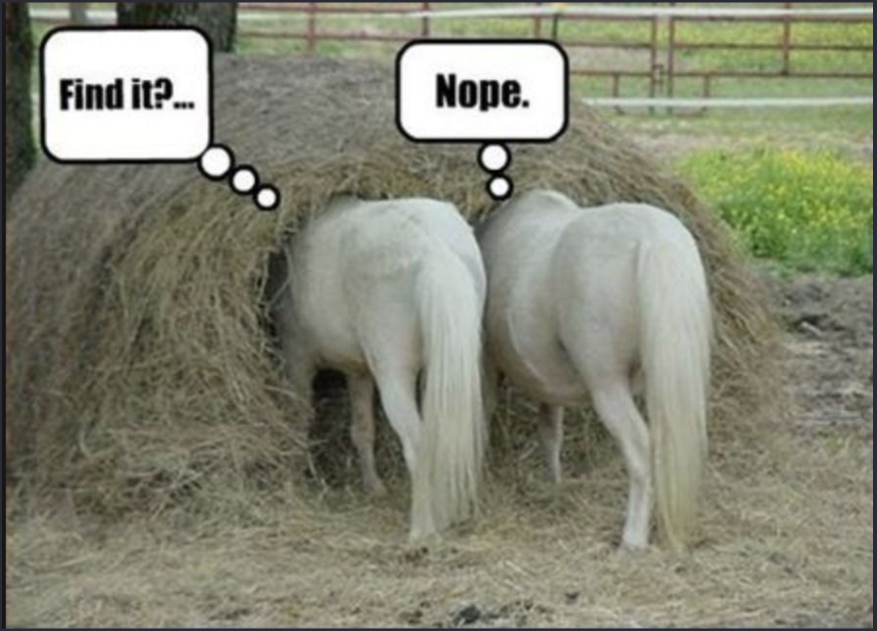
- Management Overview
- Spaces
- Index Patterns
- Beats Management

I Need My Space

- Create your own space
- Change to your space
- Create Index Patterns
  - bro-*
  - suricata-*
  - fsf-*

Kibana - Searching

Seek & Ye Shall Find



Exercise - Discover (Searching)

Kibana Searching - Basics

- Phrases
- Must {must not} be present
- Grouping
- Field matching
- Field exists {missing}
- Wildcard
- IP addresses

Kibana Searching - Advanced Exercise

- Regular expressions
- Fuzzy
- Proximity
- Numbers

Kibana Searching - Final Notes

- Saved searches
- Short URL
- _field
- .keyword

Kibana - Visualize

Pretty Pictures

Kibana Visualize - Introduction

- Basic charts
- Data
- Maps
- Time series
- Other

Kibana Visualize - Terminology

- Metrics
- Buckets

Kibana Visualize - Data

- Data Table
- Metric
- Gauge & Goal
- Pie Chart

Kibana Visualize - Data Exercise

- Top/Bottom 10 Originating Hosts
- Top/Bottom 10 Responding Hosts
- Top/Bottom 10 Originating Ports
- Top/Bottom 10 Responding Ports
- Top/Bottom 10 DNS Query
- Top/Bottom DNS Answer
- Top/Bottom HTTP Host
- Top/Bottom 10 HTTP User Agent
- Originating Hosts vs Orig IP Bytes
- Responding Hosts vs Resp IP Bytes
- DNS Authoritative Answer

- Top/Bottom 10 HTTP referrer
- CONN - Service
- CONN - State
- CONN - History
- CONN - Protocol
- HTTP Mime Type
- HTTP Status Code
- HTTP Status Msg
- DNS Protocol
- DNS Recursion Desired
- DNS Recursion Available

Kibana Visualize - Basic Charts

- Bar Chart
- Line Chart
- Area Chart
- Heat Map

Kibana Visualize - Basics Exercise

- Create the following
    - CONN - Protocols over time
    - CONN - IP ORIG/RESP Bytes over time
    - Sum of Orig IP Bytes by Originating Hosts over time
    - Sum of HTTP body length by HTTP method over time
    - DNS Response Codes over time
    - DNS Query Types over time
    - Sum of CONN IP Bytes by Protocol over time
    - Sum IP Bytes vs Sum of Bytes over time

Kibana - Dashboard

All the Pretty Pictures

Kibana Dashboard - Introduction

- Adding Visualizations
- Adding Saved Searches

Kibana Dashboard - Ideas

- Flow based dashboards
- Protocol based dashboards
- Directional traffic dashboards
- Anomaly / red flag dashboards

Kibana Dashboard - Exercise

- Build Flow Dashboard
- Build HTTP Dashboard
- Build DNS Dashboard

Kibana Dashboard - Exercise

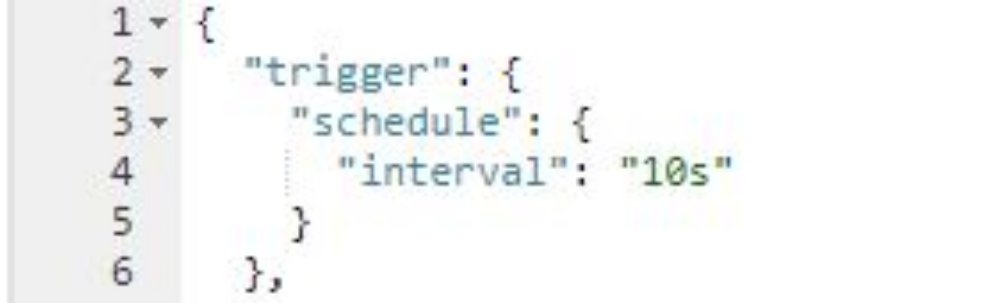
- Create new dashboards that focus on:
    - Inbound traffic
    - Outbound traffic
    - Internal traffic

Alerting

- Introduction to alerting
- Pieces of an alert
- Status of an alert

Alerting

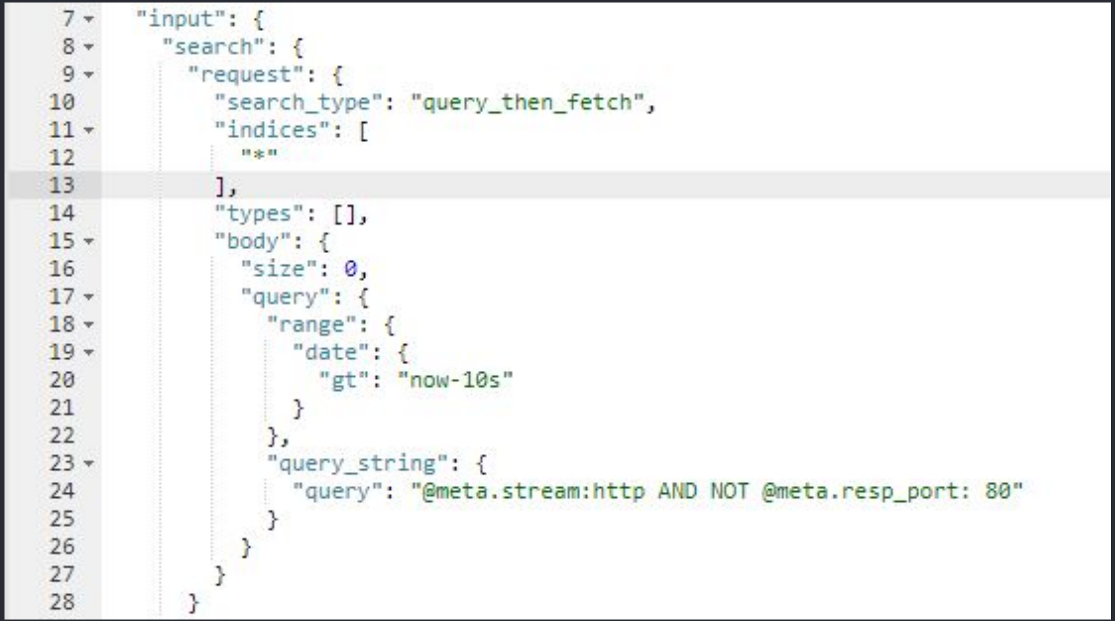
Trigger example



```
{
  "trigger": {
    "schedule": {
      "interval": "10s"
    }
  },
```

Alerting

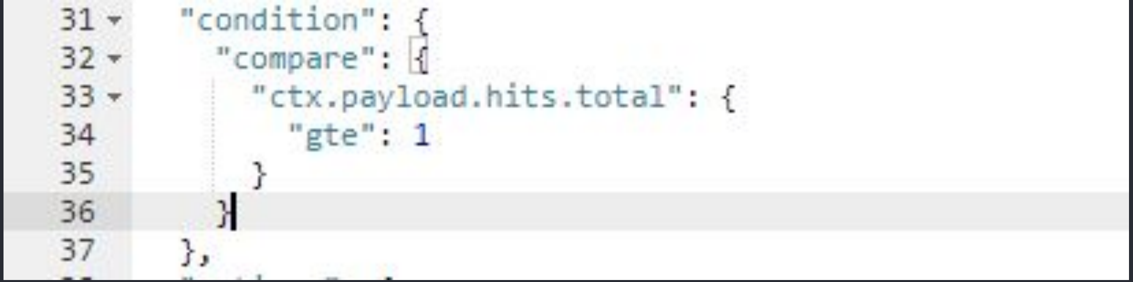
Input example



```
"input": {
  "search": {
    "request": {
      "search_type": "query_then_fetch",
      "indices": [
        "*"
      ],
      "types": [],
      "body": {
        "size": 0,
        "query": {
          "range": {
            "date": {
              "gt": "now-10s"
            }
          },
          "query_string": {
            "query": "@meta.stream:http AND NOT @meta.resp_port: 80"
          }
        }
      }
    }
```

Alerting

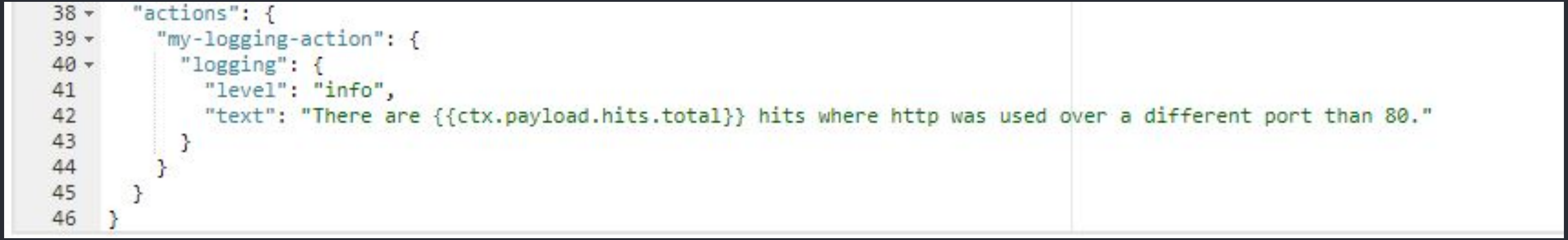
Condition example



```
"condition": {
  "compare": {
    "ctx.payload.hits.total": {
      "gte": 1
    }
  }
},
```

Alerting

Actions example



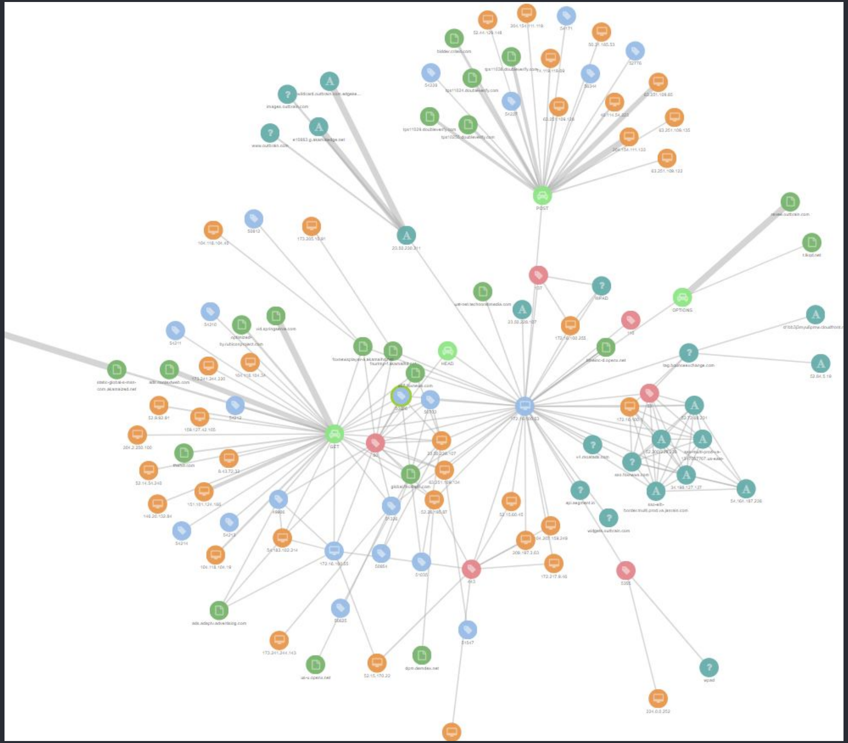
```
  "actions": {
    "my-logging-action": {
      "logging": {
        "level": "info",
        "text": "There are {{ctx.payload.hits.total}} hits where http was used over a different port than 80."
      }
    }
  }
}
```

Alerting Exercise

- Let’s make it work on the static data
- Modify your existing Alert in the following ways
  - Trigger every 10 seconds
  - Query the whole index without a time restraint
- Once you see your alert, disable your Watch

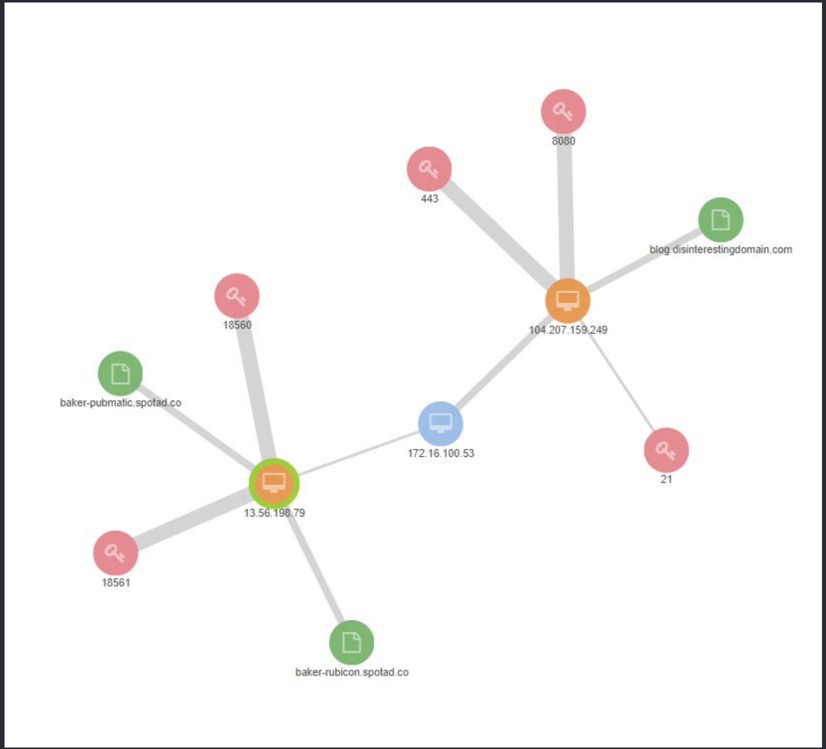
Graph

Death by bubbles

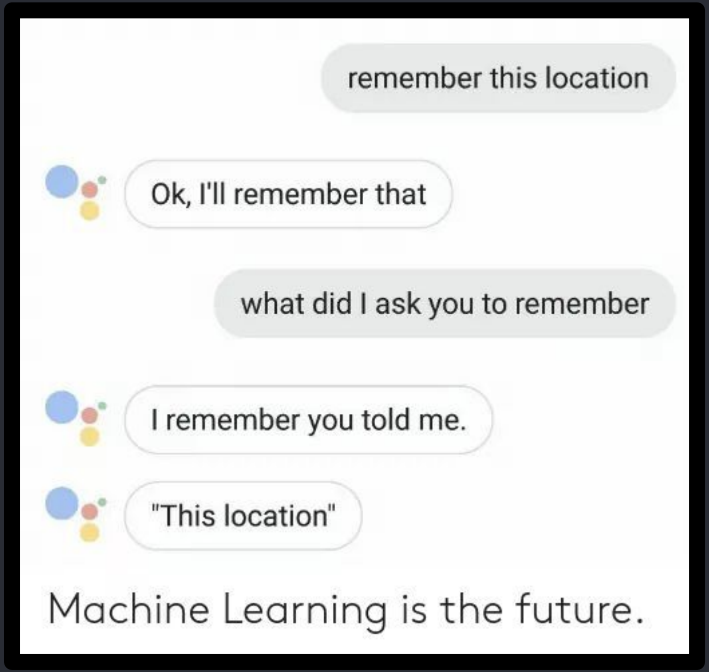


Graph

Start focused and expand



Machine Learning


remember this location

Ok, I'll remember that

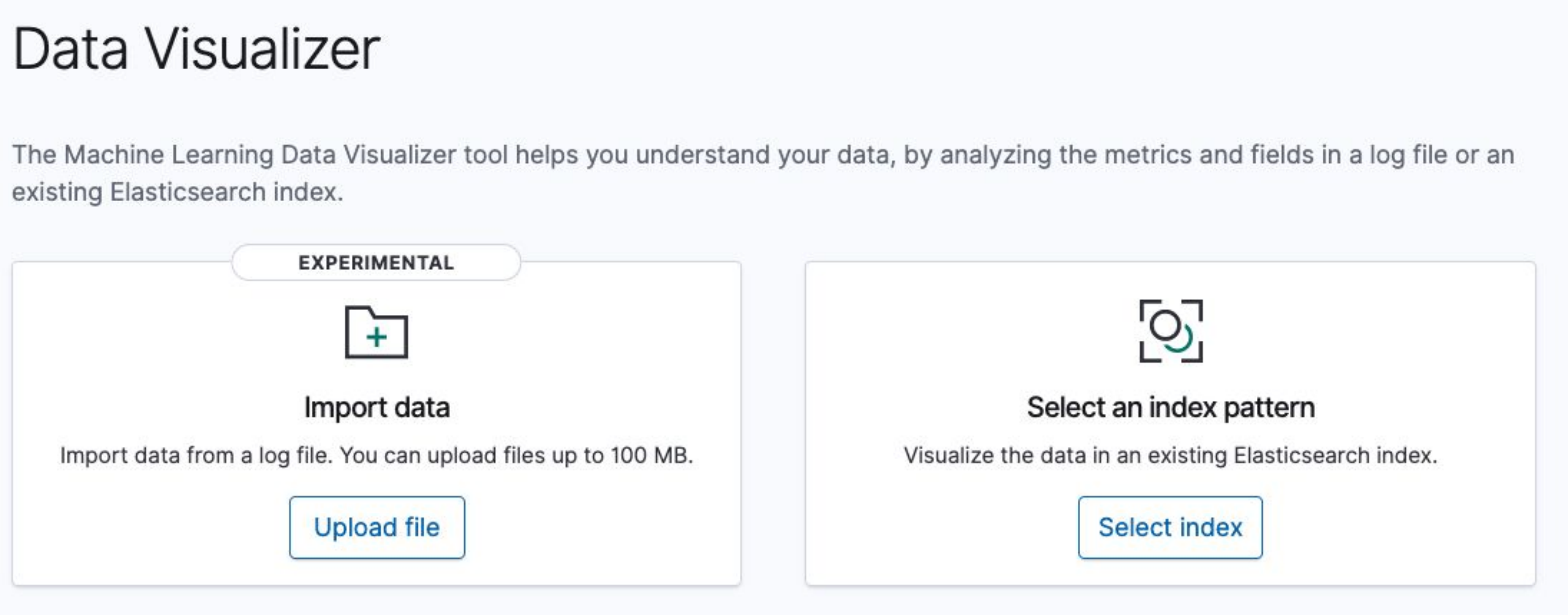
what did I ask you to remember

I remember you told me.

"This location"

Machine Learning is the future.

Machine Learning - Exploring data



Data Visualizer

The Machine Learning Data Visualizer tool helps you understand your data, by analyzing the metrics and fields in a log file or an existing Elasticsearch index.

Import data from a log file. You can upload files up to 100 MB.

Visualize the data in an existing Elasticsearch index.

Hunting with Kibana

- Bringing it all together