Elastic Stack for Security Monitoring in a Nutshell

2019 Pass the SALT Workshop

ALZETTE INFORMATION SECURITY

Overview

- Introduction to Elastic Stack
- Beats
- Logstash
- Elasticsearch
- Kibana
- Elastic Stack Alerting and Security

Introductory Workshop!

- This is an introductory workshop
- You probably won’t hear/see a lot of new things if you have:
  - Used Elastic Stack in the past;
  - Took the Elastic training…;
  - Followed SANS SEC455, SEC555, FOR572, etc.;
- **If you are stuck, please do not suffer in silence!**

Workshop VM

- ais_workshop_xubuntu-18.04.2-desktop-amd64
- VMware Workstation, Player, or Fusion
  - You can try VirtualBox too, but you are on your own with that… sorry! ☺
- 8 GB RAM
- 30-50 GB disk space
- **Keyboard layout: EN-US !!!**
- Workshop VM (Ubuntu) user/pass: **user / Workshop1234%**
  - Normally, it should not require password for login and sudo

About David

- Managing partner at Alzette Information Security (@AlzetteInfoSec)
- Network penetration testing, security architectures, security monitoring, incident response
- Instructor at SANS Institute: FOR572
- BSides Luxembourg organizer https://bsideslux.lu
- Twitter: @DavidSzili
- E-mail: david.szili@alzetteinfosec.com
- Blog: http://jumpespjump.blogspot.com

About Eva

- Managing partner at Alzette Information Security (@AlzetteInfoSec)
- Web application penetration testing, source code review, security monitoring
- CyberWayFinder
- BSides Luxembourg organizer https://bsideslux.lu
- Twitter: @EvaSzilagyiSec
- E-mail: eva.szilagyi@alzetteinfosec.com
- Blog: http://jumpespjump.blogspot.com

Introduction to Elastic Stack

7

2019 Pass the SALT Workshop

ALZETTE INFORMATION SECURITY

About Elastic Stack

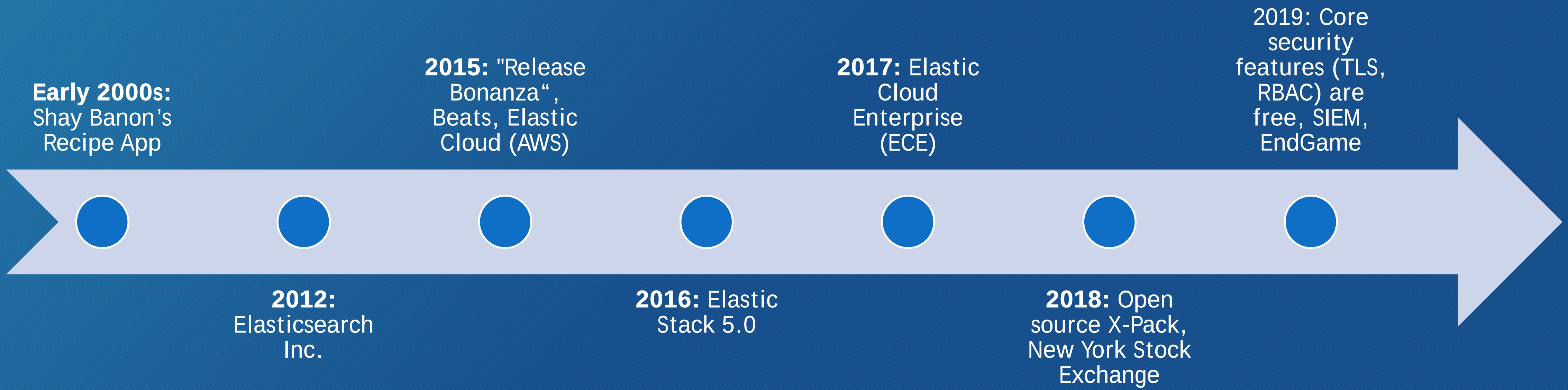
What is Elastic Stack?

- 4 main components:
  - Elasticsearch
  - Logstash
  - Kibana
  - Beats
- And several other smaller components
  - Elastic Stack Features (X-Pack)
  - APM (Application Performance Monitoring)

Why Elastic Stack?

- (Free) Open Source Software
- Distributed, real-time search and analytics (very scalable)
- Parsing and data enrichment
- Large Community
- InfoSec Projects built around it:
  - Security Onion
  - Moloch (Elasticsearch)
  - SOF-ELK
  - SELKS
  - HELK
  - ROCK NSM

Elastic Stack History



Early 2000s: Shay Banon’s Recipe App

2012: Elasticsearch Inc.

2015: "Release Bonanza“, Beats, Elastic Cloud (AWS)

2016: Elastic Stack 5.0

2017: Elastic Cloud Enterprise (ECE)

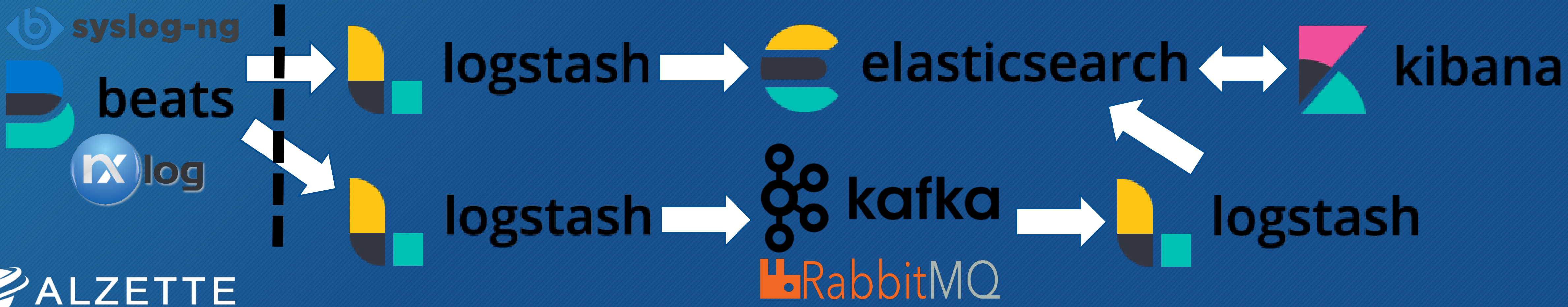
2018: Open source X-Pack, New York Stock Exchange

2019: Core security features (TLS, RBAC) are free, SIEM, EndGame

Source: https://www.elastic.co/about/history-of-elasticsearch

Elastic Stack (Very) High-Level Overview

- **Beats**: single-purpose data shippers
- **Logstash**: server-side data processing pipeline
- **Elasticsearch**: distributed search and analytics engine
- **Kibana**: visualization and dashboards



See also: https://www.elastic.co/assets/blt2614227bb99b9878/architecture-best-practices.pdf

Beats

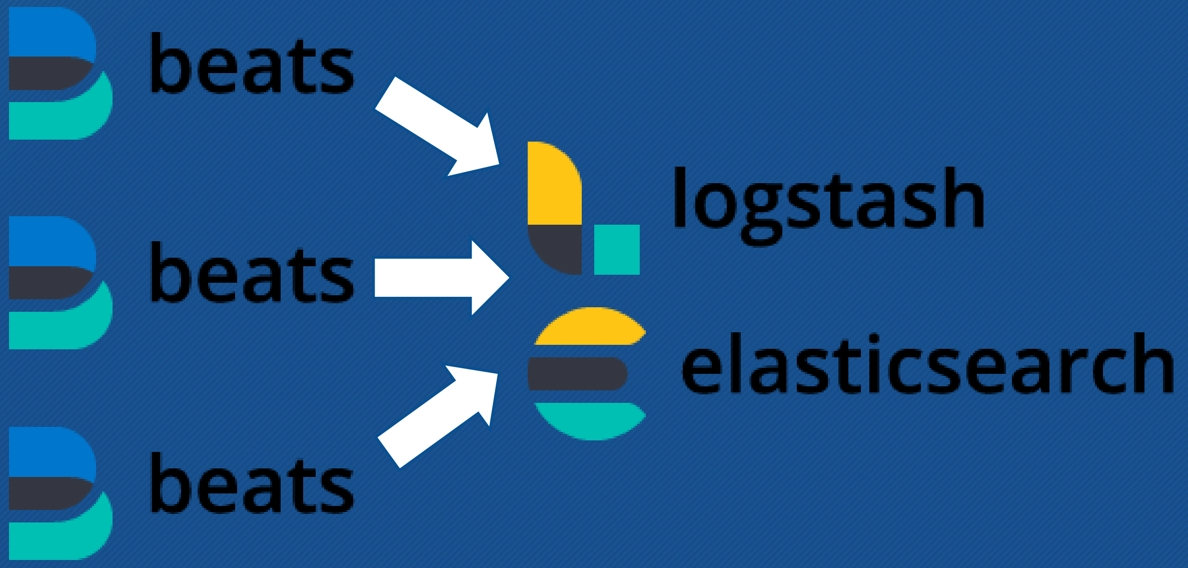
11

2019 Pass the SALT Workshop

ALZETTE INFORMATION SECURITY

Beats: Lightweight Data Shippers

- Lightweight log agents
- Written in Go
- Can send to Logstash or directly to Elasticsearch
- Beats Family:
  - **Filebeat**
  - **Winlogbeat**
  - **Auditbeat**
  - Packetbeat
  - Heartbeat
  - Metricbeat
  - Functionbeat
  - Etc.

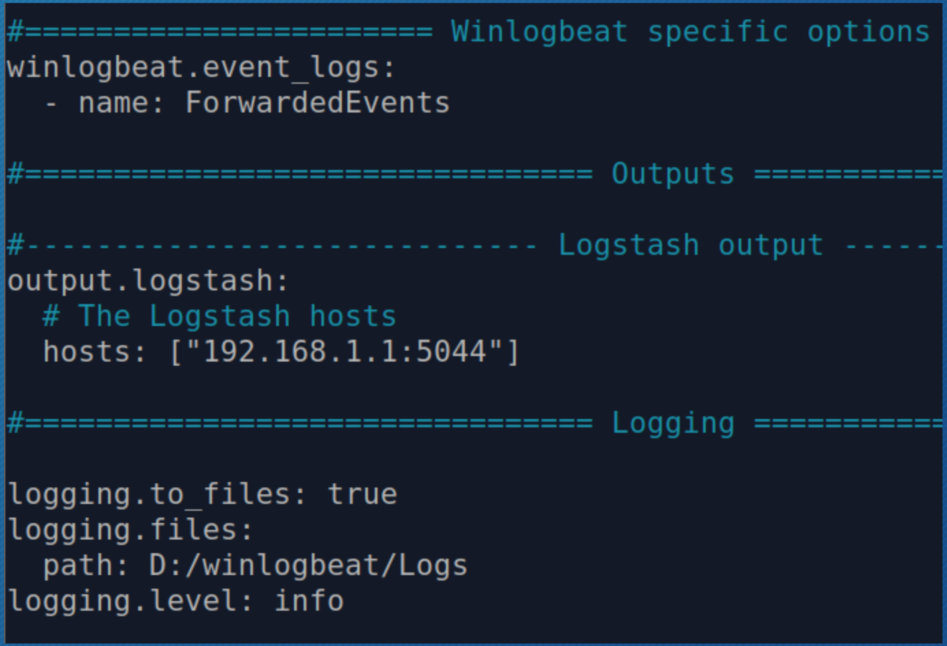


ALZETTE INFORMATION SECURITY

See also: https://www.elastic.co/guide/en/beats/libbeat/current/index.html

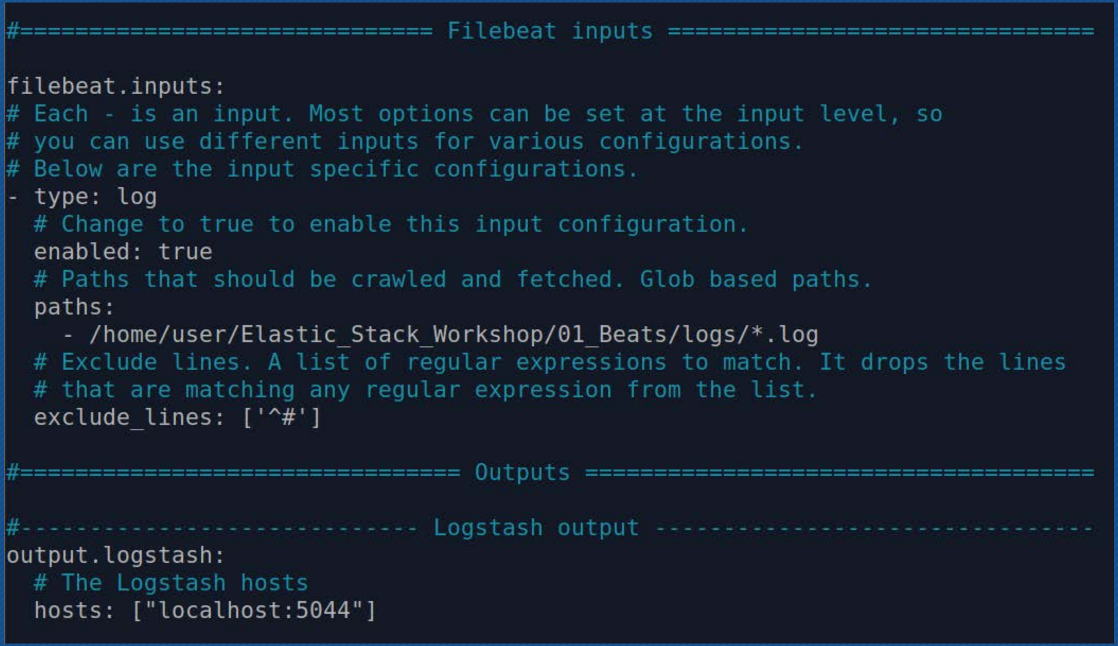
Beats Configuration Examples

Winlogbeat



```
#======================== Winlogbeat specific options
winlogbeat.event_logs:
  - name: ForwardedEvents

#================================ Outputs ==========

#----------------------------- Logstash output -----
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.1.1:5044"]

#================================ Logging ==========

logging.to_files: true
logging.files:
  path: D:/winlogbeat/Logs
logging.level: info
```

Filebeat



```
#=============================== Filebeat inputs ===============================

filebeat.inputs:
# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.
- type: log
  # Change to true to enable this input configuration.
  enabled: true
  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /home/user/Elastic_Stack_Workshop/01_Beats/logs/*.log
  # Exclude lines. A list of regular expressions to match. It drops the lines
  # that are matching any regular expression from the list.
  exclude_lines: ['^#']

#================================= Outputs ====================================

#----------------------------- Logstash output --------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]
```

Beats Hands-On

14

2019 Pass the SALT Workshop

ALZETTE

INFORMATION SECURITY

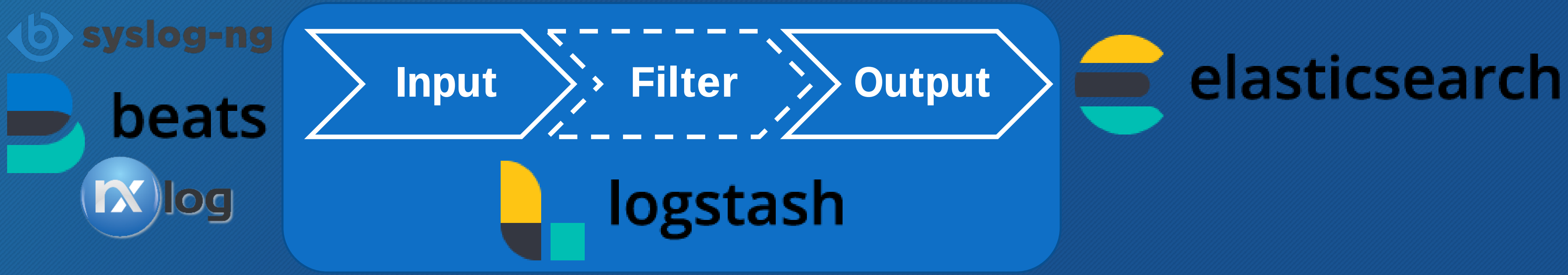
Logstash

15

2019 Pass the SALT Workshop

Logstash Overview

- **LOTS AND LOTS** of plugins!
  - **Input**: tcp, udp, **syslog**, **beats**, **jdbc**, kafka, rabbitmq, **file**, exec, cloudwatch, etc.
  - **Filter**: **csv**, **json**, **xml**, **kv**, **grok**, **date**, **mutate**, split, useragent, ruby, **drop**, etc.
  - **Output**: **elasticsearch**, graphite, nagios, kafka, rabbitmq, radis, file, **email**, irc, etc.
- Easy to learn and use



See also: https://www.elastic.co/guide/en/logstash/current/index.html

Input Plugin Examples

Plugin	Description
beats	Events from Elastic Beats
cloudwatch	Events from AWS CloudWatch
file	Streams events from files
jdbc	Events from JDBC data
kafka	Reads events from Kafka
rabbitmq	Pulls events from RabbitMQ
s3	Events from files in S3
snmp	Polls devices using SNMP
syslog	Reads syslog messages

```
input {
    stdin {
    }
}
```

```
input {
    beats {
        port => 5044
    }
}
```

```
input {
    syslog {
        port => 5514
    }
}
```

ALZETTE
INFORMATION SECURITY

See also: https://www.elastic.co/guide/en/logstash/current/input-plugins.html

Filter Plugin Examples

Plugin	Description
cidr	Check IP against net blocks
csv	Parses CSV data into fields
date	Parses dates from fields
dissect	Extracts unstructured data
drop	Drops all events
elasticsearch	Gets data from Elasticsearch
geoip	Geo info about an IP
grok	Parses unstructured data
json	Parses JSON data

Plugin	Description
kv	Parses key-value pairs
mutate	Performs mutations on fields
ruby	Executes Ruby code
split	Splits multi-line messages
translate	Replaces field contents
truncate	Truncates fields
urldecode	Decodes URL-encoded fields
useragent	Parses user agent strings
xml	Parses XML data

See also: https://www.elastic.co/guide/en/logstash/current/filter-plugins.html

Filters - The Easy Stuff

JSON

```
filter {
    ...
    json {
        source => "message“
    }
    ...
    mutate {
        remove_field => [ "message" ]
    }
}
```

CSV

```
filter {
    ...
    csv {
        columns => ["ts", "uid", "id.orig_h",
"id.orig_p", "id.resp_h", "id.resp_p", "proto",
"service", "duration", "orig_bytes",
"resp_bytesconn_state", "local_orig", "local_resp",
"missed_bytes", "history", "orig_pkts", "orig_ip_bytes",
"resp_pkts", "resp_ip_bytes", "tunnel_parents"]
        separator => "    “
    }
    ...
    mutate {
        remove_field => [ "message" ]
    }
}
```

ALZETTE
INFORMATION SECURITY

Filters - RegExp vs. Grok, Dissect (1)

RegExp

- (?<![0-9])(?:(?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]{1,2})[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]{1,2})[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]{1,2})[.](?:25[0-5]|2[0-4][0-9]|[0-1]?[0-9]{1,2}))(?![0-9])

Dissect

- String-based split operation
- Very fast

Grok

- %{IPV4:source_ip}
- Pre-cooked RegExp patterns
- Custom Patterns:
  - (?<queue_id>[0-9A-F]{10,11})

Grok Debuggers:

- Heroku App: http://grokdebug.herokuapp.com
- Source: https://github.com/nickethier/grokdebug
- Docker: https://hub.docker.com/r/fdrouet/grokdebug
- Kibana / Dev Tools / Grok Debugger

ALZETTE
INFORMATION SECURITY

Filters - RegExp vs. Grok, Dissect (2)

dissect

```
filter {
    ...
    dissect {
        mapping => {
            "message" => "%{ts} %{+ts}
%{+ts} %{src} %{prog}[%{pid}]: %{msg}“
        }
    }
    ...
}
```

grok

```
filter {
    ...
    grok {
        match => {
            "message" =>
"%{SYSLOGTIMESTAMP:syslog_timestamp}
%{SYSLOGHOST:syslog_hostname}
%{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?:
%{GREEDYDATA:syslog_message}"

            #"message" => "%{SYSLOGBASE2}
%{GREEDYDATA:message}“
        }
    }
    ...
}
```

Filters - Enrichment Examples

ruby

```
filter {
    ...
    if [program] == "bro_dns" {
        ruby {
            code => "event.set('query_length',
event.get('query').length)“
        }
    }
    ...
}
```

geoip

```
filter {
    ...
    if [resp_h_routable] == "true" {
        geoip {
            source => "id.resp_h“
            target => "geoip“
            default_database_type => "City“
        }
        geoip {
            source => "id.resp_h“
            target => "geoip“
            default_database_type => "ASN“
        }
    }
    ...
}
```

Output Plugin Examples

Plugin	Description
csv	Writes events to disk in CSV
elasticsearch	Stores logs in Elasticsearch
email	Sends email to an address
exec	Runs a command
file	Writes events to files
graphite	Writes metrics to Graphite
kafka	Writes events to Kafka
rabbitmq	Pushes events to RabbitMQ
redis	Sends events to Redis

```
output {
    stdout {
        codec => rubydebug
    }
}
```

```
output {
    elasticsearch {
        hosts => ["localhost:9200"]
    }
}
```

See also: https://www.elastic.co/guide/en/logstash/current/output-plugins.html

Elastic Common Schema (ECS)

- Specification that provides a consistent and customizable way to structure your data in Elasticsearch
  - Searches can be created more narrowly
  - Field names are easier to remember
- ECS Reference: https://www.elastic.co/guide/en/ecs/current/index.html
- ECS GitHub: https://github.com/elastic/ecs

Level	Description
ECS Core Fields	Fully defined set of field names that exists under a defined set of ECS top-level objects
ECS Extended Fields	Partially defined set of field names that exists under the same set of ECS top-level objects
Custom Fields	Undefined and unnamed set of fields that exists under a user-supplied set of non-ECS top-level objects that must not conflict with ECS fields or objects

Logstash Hands-On

2019 Pass the SALT Workshop

ALZETTE

INFORMATION SECURITY

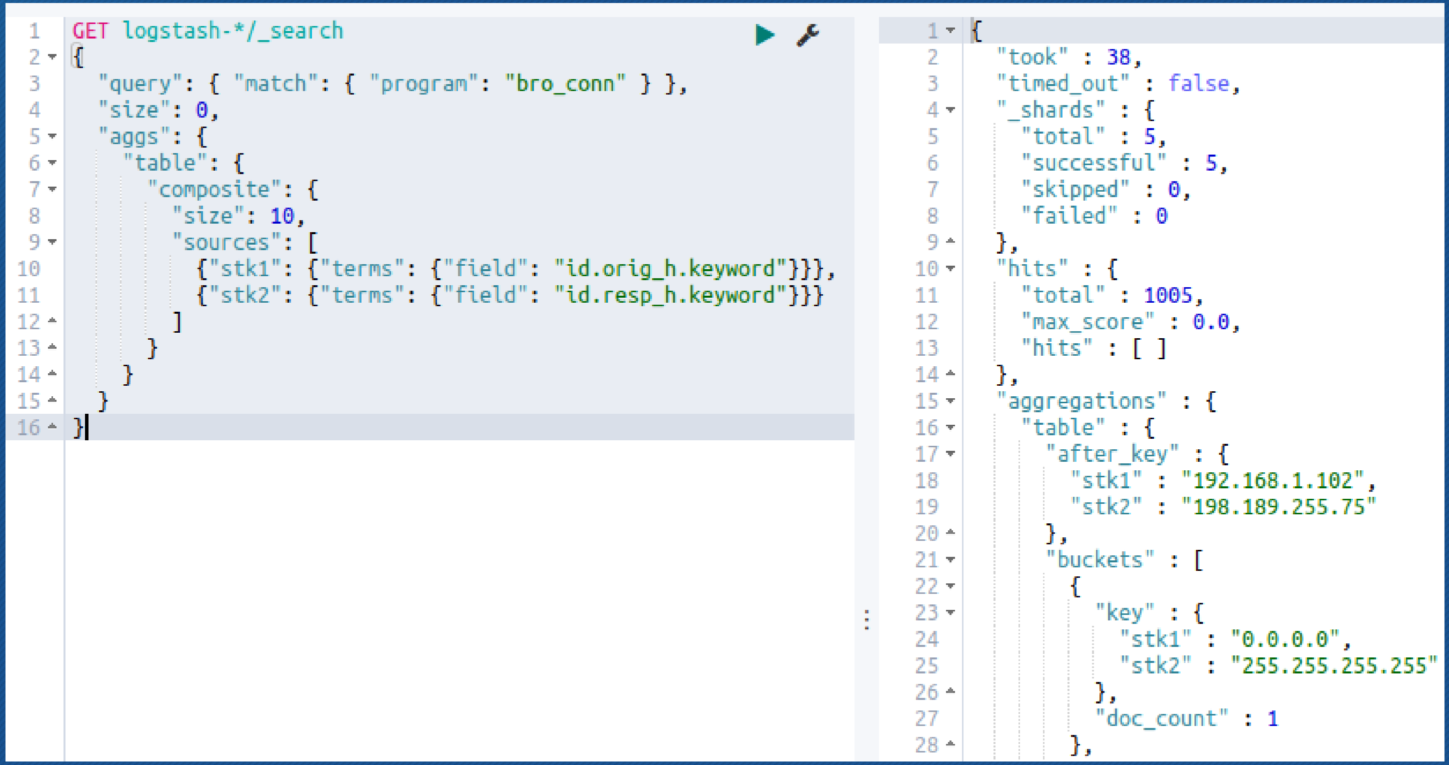
Elasticsearch

2019 Pass the SALT Workshop

Elasticsearch Overview

- Storage and Search
- Built on Apache Lucene
  - “wrapper” written in Java
- REST API
- JSON over HTTP
- Distributed
- Real-time

More info: **John Hubbard - The Elastic Stack as a SIEM:** **https://www.youtube.com/watch?v=v69kyU5XMFI**

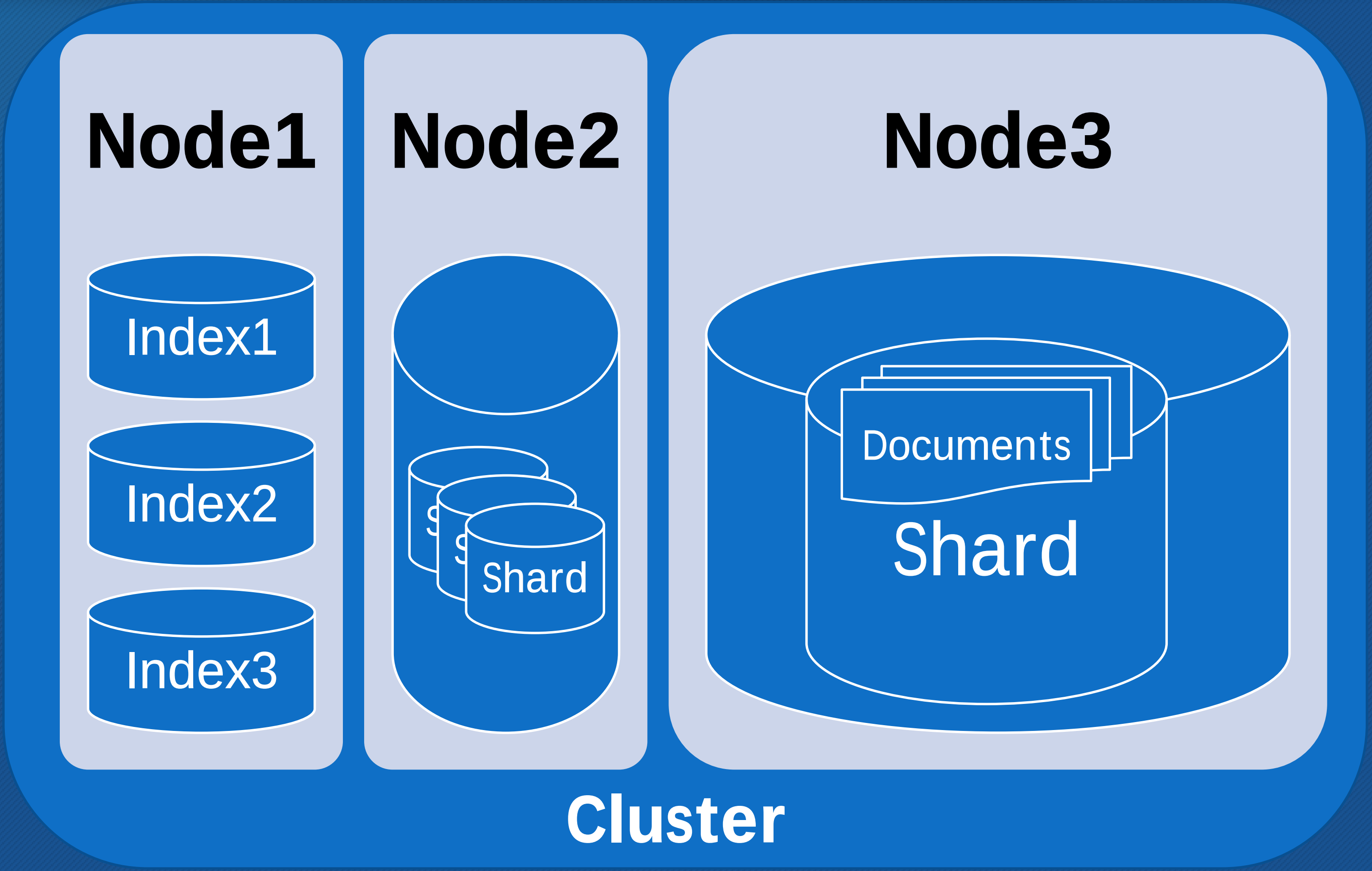


```
GET logstash-*/_search
{
  "query": { "match": { "program": "bro_conn" } },
  "size": 0,
  "aggs": {
    "table": {
      "composite": {
        "size": 10,
        "sources": [
          {"stk1": {"terms": {"field": "id.orig_h.keyword"}}},
          {"stk2": {"terms": {"field": "id.resp_h.keyword"}}}
        ]
      }
    }
  }
}
```

```
{
  "took" : 38,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : 1005,
    "max_score" : 0.0,
    "hits" : [ ]
  },
  "aggregations" : {
    "table" : {
      "after_key" : {
        "stk1" : "192.168.1.102",
        "stk2" : "198.189.255.75"
      },
      "buckets" : [
        {
          "key" : {
            "stk1" : "0.0.0.0",
            "stk2" : "255.255.255.255"
          },
          "doc_count" : 1
        },
```

Elasticsearch Terms

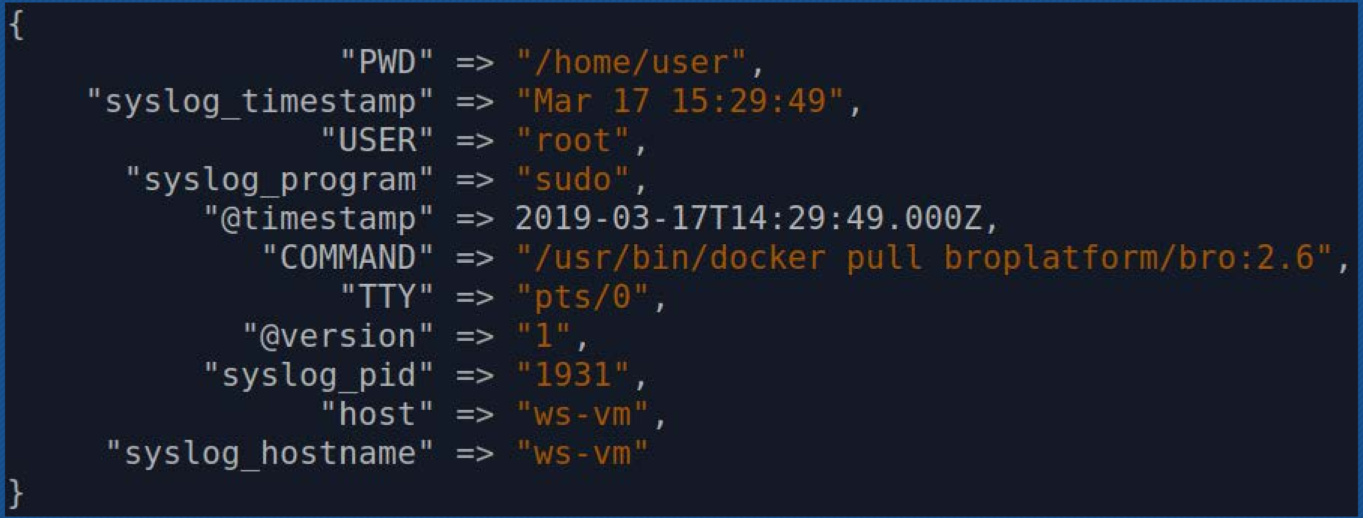
- **Cluster**: All nodes
- **Node**: Elasticsearch instance
- **Index**: Set of documents (group of shards)
- **Shard**:
  - Subset of documents in an index
  - Apache Lucene instance
  - Primary (like RAID 0) and Replica (like RAID 1)
- **Document**: JSON object in Elasticsearch



Elasticsearch vs. Relational Database

- **Mapping**:
  - Defines field names and datatypes in documents
  - Can add new fields, but existing fields cannot be changed!
- **Field**:
  - Key-value pair in a document
  - Metadata like: _index, _id, etc.
- **WORM** (Write Once Read Many) vs. **ACID** (Atomicity, Consistency, Isolation, Durability)

Elasticsearch	Relational Database
Index	Database
Mapping	Schema
Document	Row
Field	Column



```
{
                 "PWD" => "/home/user",
    "syslog_timestamp" => "Mar 17 15:29:49",
                "USER" => "root",
      "syslog_program" => "sudo",
          "@timestamp" => 2019-03-17T14:29:49.000Z,
             "COMMAND" => "/usr/bin/docker pull broplatform/bro:2.6",
                 "TTY" => "pts/0",
            "@version" => "1",
          "syslog_pid" => "1931",
                "host" => "ws-vm",
     "syslog_hostname" => "ws-vm"
}
```

Data Types (Few Examples)

Core

- ***text***
- ***keyword***
- long, ***integer***, short, byte
- double, float, half_float, scaled_float
- ***boolean***
- binary

Geo

- ***geo_point***
- geo_shape

Specialized

- ***date***
- ***ip***

Complex

- ***array***
- object
- nested

Multi-fields

- Indexed as more one type

Etc.

See also: https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping-types.html

Text vs. Keyword

Text type

- “Full-text value”
- Payload, message, etc.
- Analyzed and **tokenized**
- **Cannot be used for**
  - Sorting
  - Aggregations

Keyword type

- “Exact value”
- IP, port, protocol, user, etc.
- Exact match / not match
- **Can be used for**
  - Sorting
  - Aggregations

Elasticsearch Hands-On

2019 Pass the SALT Workshop

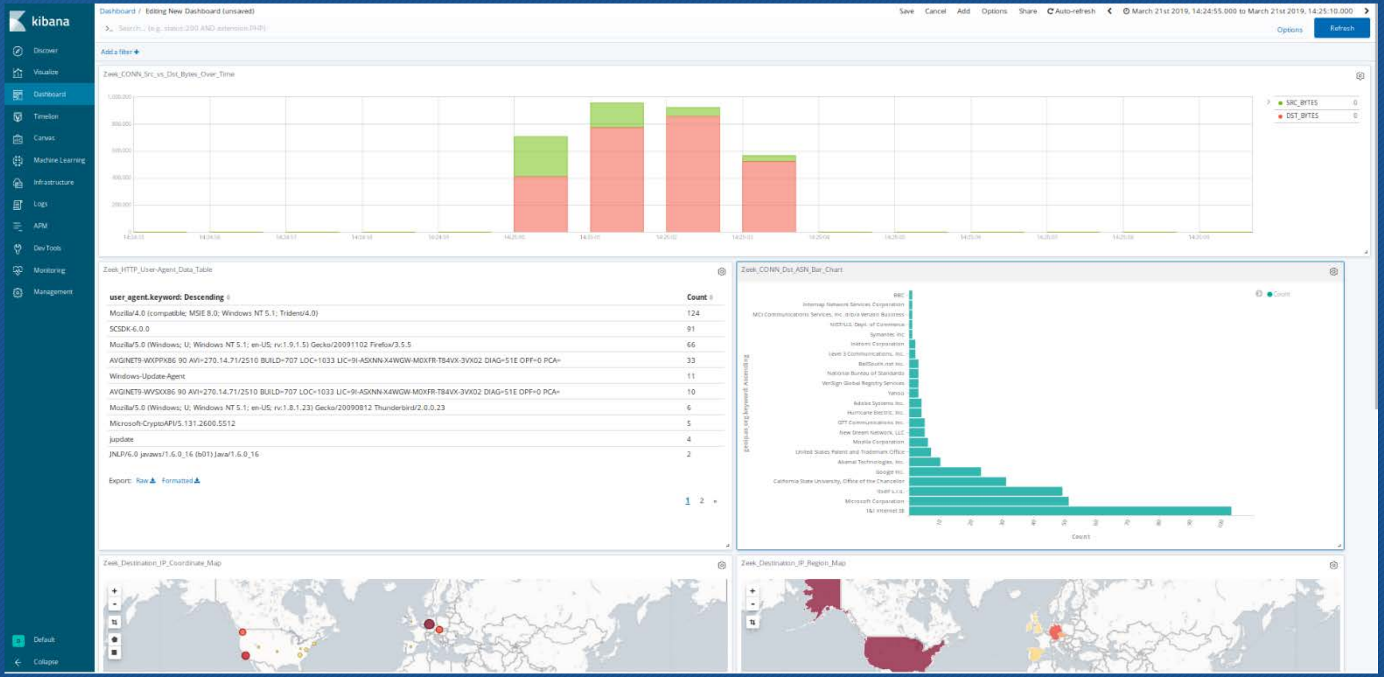
Kibana

2019 Pass the SALT Workshop

ALZETTE INFORMATION SECURITY

Kibana Overview

- Web-based analytic interface
- Searches
  - Apache Lucene syntax
- Filters
- Visualizations, Dashboards
  - Stored in JSON
- Plugins
  - Reporting, Alerting, etc.


kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Default
Collapse
Dashboard / Editing New Dashboard (unsaved)
Save
Cancel
Add
Options
Share
Auto-refresh
March 21st 2019, 14:24:55.000 to March 21st 2019, 14:25:10.000
Search... (e.g. status:200 AND extension:PHP)
Options
Refresh
Add a filter +
Zeek_CONN_Src_vs_Dst_Bytes_Over_Time
SRC_BYTES 0
DST_BYTES 0
Zeek_CONN_Dst_ASN_Bar_Chart
Count
BBC
Internap Network Services Corporation
MCI Communications Services, Inc. d/b/a Verizon Business
NIST/U.S. Dept. of Commerce
Symantec Inc
Inktomi Corporation
Level 3 Communications, Inc.
BellSouth.net Inc.
National Bureau of Standards
VeriSign Global Registry Services
Yahoo
Adobe Systems Inc.
Hurricane Electric, Inc.
GTT Communications Inc.
New Dream Network, LLC
Mozilla Corporation
United States Patent and Trademark Office
Akamai Technologies, Inc.
Google Inc.
California State University, Office of the Chancellor
Itself s.r.o.
Microsoft Corporation
1&1 Internet SE
geoip.as_org.keyword: Ascending
Zeek_Destination_IP_Coordinate_Map
Zeek_Destination_IP_Region_Map

Zeek_HTTP_User-Agent_Data_Table

user_agent.keyword: Descending	Count
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	124
SCSDK-6.0.0	91
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5	66
AVGINET9-WXPPX86 90 AVI=270.14.71/2510 BUILD=707 LOC=1033 LIC=9I-ASXNN-X4WGW-M0XFR-T84VX-3VX02 DIAG=51E OPF=0 PCA=	33
Windows-Update-Agent	11
AVGINET9-WVSXX86 90 AVI=270.14.71/2510 BUILD=707 LOC=1033 LIC=9I-ASXNN-X4WGW-M0XFR-T84VX-3VX02 DIAG=51E OPF=0 PCA=	10
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.23) Gecko/20090812 Thunderbird/2.0.0.23	6
Microsoft-CryptoAPI/5.131.2600.5512	5
jupdate	4
JNLP/6.0 javaws/1.6.0_16 (b01) Java/1.6.0_16	2

Export: Raw Formatted

1 2 »

Kibana Features

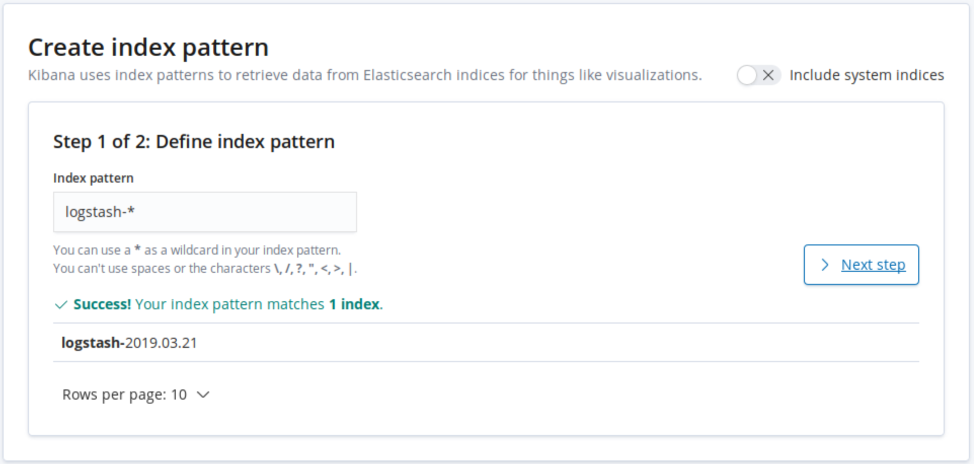
- **Discover**: Search
- **Visualize**: Graphs, charts
  - Vega, Vega-Lite
- **Dashboard**: Visualizations and saved searches
- **Timelion**: Time series visualizations
- **Canvas**: Presentation
- **Machine Learning** (Paid)
- **Graph** (Paid)
- **Infrastructure**: Metricbeats monitoring
- **Logs**: Filebeat monitoring
- **APM**: Application Performance Monitoring
- **Uptime**: Monitor the status of network endpoints
- **SIEM:** Interactive workspace for security investigations
- **Dev Tools**: API access
- **Monitoring**: Cluster health
- **Management**: Cluster management
- etc.

Index Patterns

- Must choose an index pattern
  - Discovery (Searches)
  - Visualization
- Limits the indices searched
- Relates to index naming scheme
- Can use the * wildcard
  - “logstash-* ”

Steps:

1. Create Elasticsearch index
2. “Create index pattern”
3. Select index/indices
4. Define @timestamp field



Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

☒ Include system indices

Step 1 of 2: Define index pattern

Index pattern: logstash-*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

✓ **Success!** Your index pattern matches **1 index**.

logstash-2019.03.21

Rows per page: 10

Search – Apache Lucene Query Syntax (1)

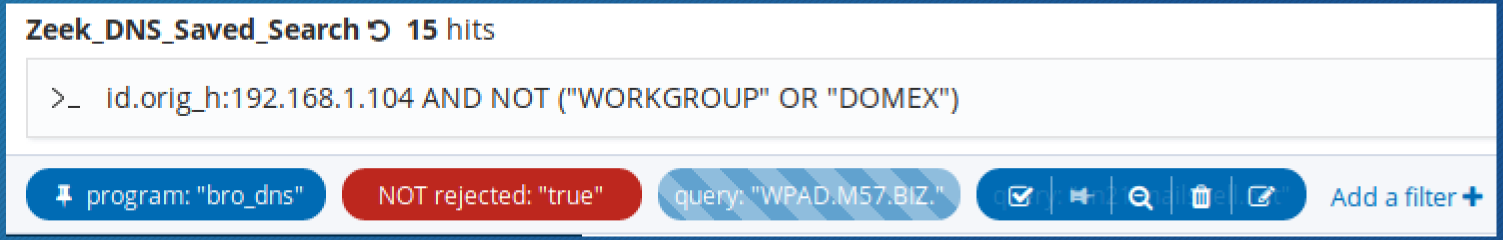
Search Type	Syntax	Example
Single Term	<term>	hello
Phrase	“<term>”	“hello world”
Fields	<field>:<term>	title:hello
AND	<term-a> AND <term-b>	hello AND world // hello world
OR	<term-a> OR <term-b>	hello OR world
NOT	NOT <term-a> !<term-a>	NOT “hello world” !“hello world”
Must match	+<term>	+hell!o
Must not match	-<term>	-hello

Search – Apache Lucene Query Syntax (2)

Search Type	Syntax	Example
Field exists	_exists_:<field>	_exists_:title
Field does not exists	NOT _exists_:<field> ! _exists_:<field> -_exists_:<field>	NOT _exists_:title ! _exists_:title -_exists_:title
Wildcard search	?, *	h?llo, hell*
Fuzzy search	<term>~[<number>]	hello~2
Proximity search	“<term>”~[<number>]	“hello world”~5
Range	<field>:[<value-a> TO <value-b>] <field>:{<value-a> TO <value-b>}	port:[1 TO 1024] title:{hello TO world}

Search vs. Filters And Time Range

- **Search**: Using the Query bar and the Apache Lucene Query Syntax
- **Filter**: Using the Filters Box and the Elasticsearch Query DSL (Domain Specific Language)



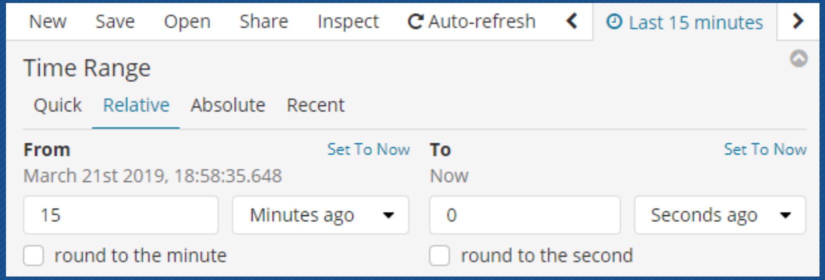
Zeek_DNS_Saved_Search ⟲ **15** hits

```
>_ id.orig_h:192.168.1.104 AND NOT ("WORKGROUP" OR "DOMEX")
```

program: "bro_dns"

NOT rejected: "true"

query: "WPAD.M57.BIZ."



From: March 21st 2019, 18:58:35.648

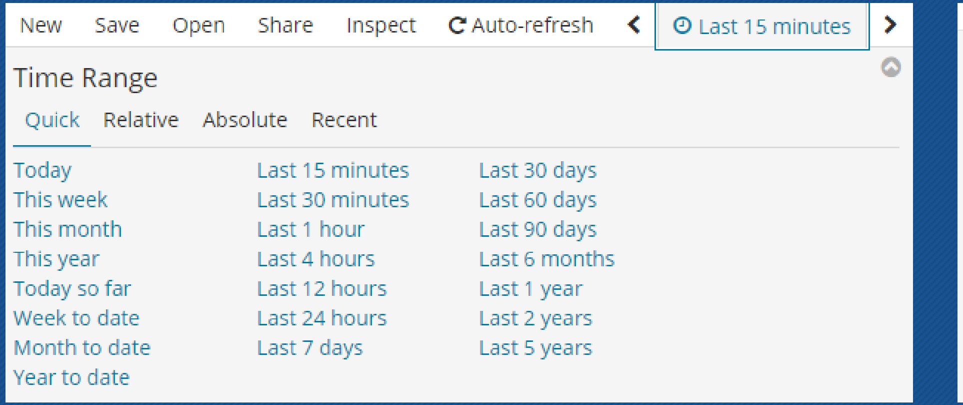
15 | Minutes ago

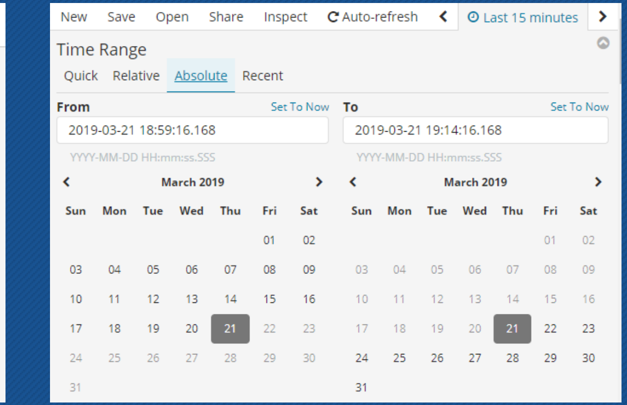
□ round to the minute

To: Now

0 | Seconds ago

□ round to the second





From: 2019-03-21 18:59:16.168

To: 2019-03-21 19:14:16.168

Visualizations

Visualization	Type
Area	Basic Charts
Heat Map	Basic Charts
Horizontal Bar	Basic Charts
Line	Basic Charts
Pie	Basic Charts
Vertical Bar	Basic Charts
Data Table	Data
Gauge	Data
Goal	Data

Visualization	Type
Metric	Data
Coordinate Map	Maps
Region Map	Maps
Timelion	Time Series
Visual Builder (E)	Time Series
Controls (E)	Other
Markdown	Other
Tag Cloud	Other
Vega (E)	Other

Visualizations use Elasticsearch Aggregations

Metrics: value to calculate

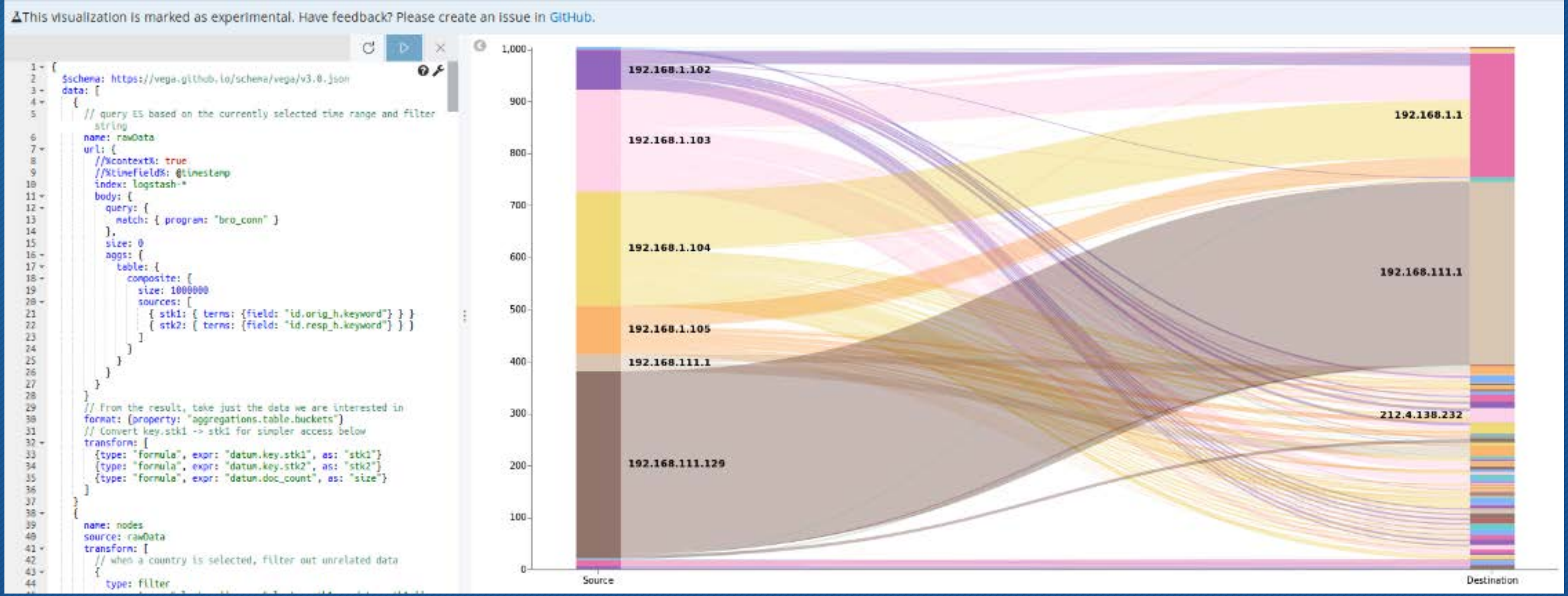
- **Count**
- **Average**
- **Sum**
- Min
- Max
- Unique Count
- **Standard Deviation**
- Top Hit
- Percentiles
- etc.

Bucket: aggregation (grouping)

- **Date Histogram** (by time)
- Date Range
- Filter
- Geo Distance
- IP Range
- Range
- Sampler
- Significant Text
- **Terms** (by field)
- etc.

Vega and VegaLite

- Vega Graphs
  - Visualization grammar
  - Declarative language
  - JSON format
- Supported from Elastic 6
- Vega vs VegaLite
  - VegaLite: simplified Vega
  - https://vega.github.io/vega/
  - https://vega.github.io/vega-lite/

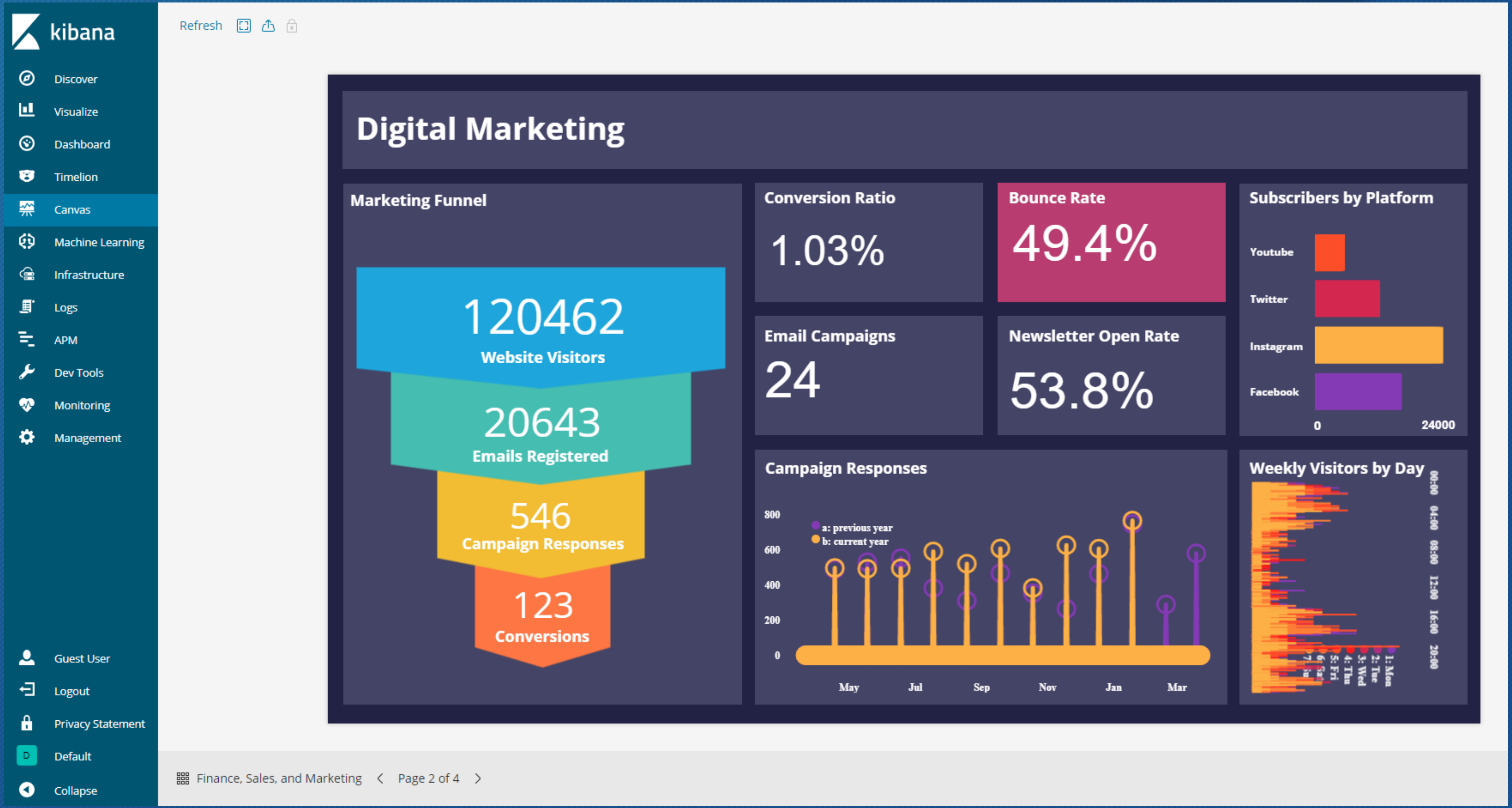


This visualization is marked as experimental. Have feedback? Please create an issue in GitHub.

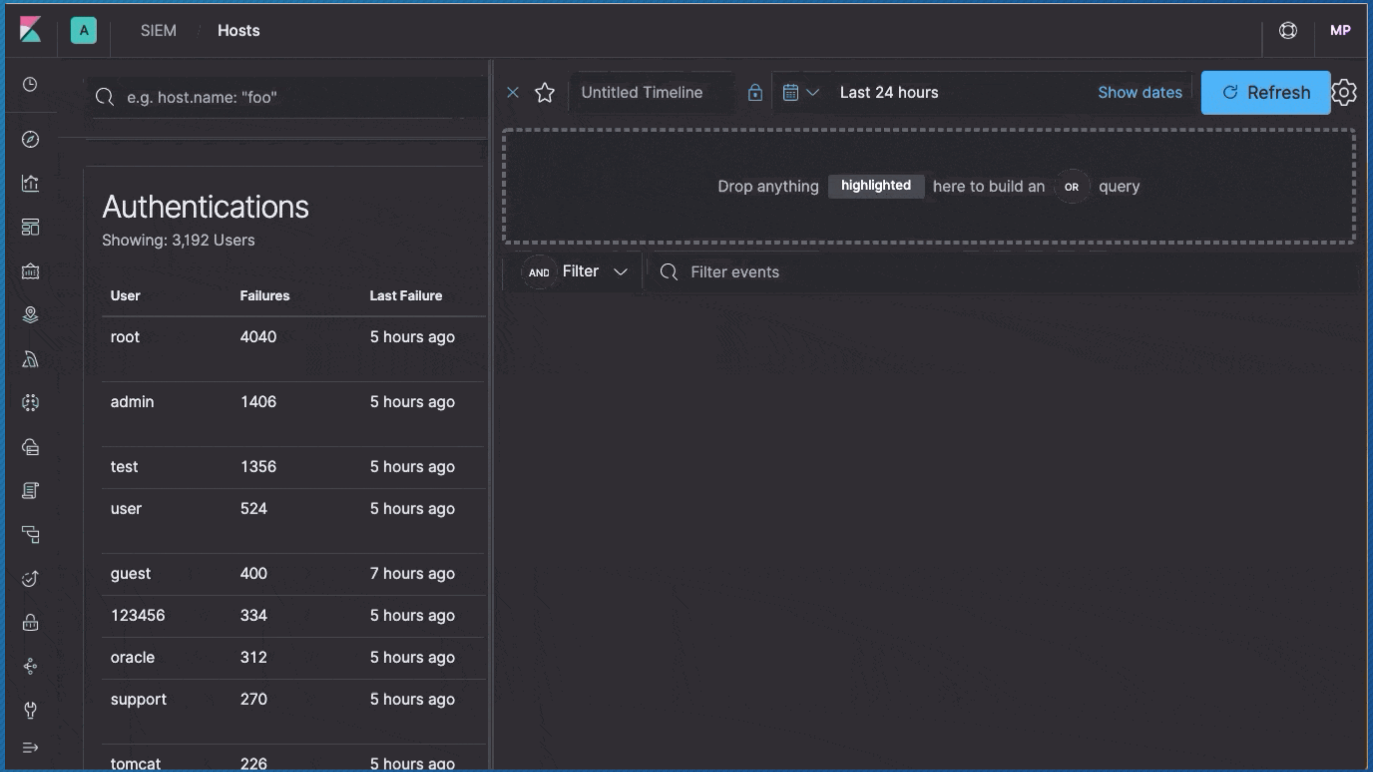
```
{
  $schema: https://vega.github.io/schema/vega/v3.0.json
  data: [
    {
      // query ES based on the currently selected time range and filter
        string
      name: rawData
      url: {
        //%context%: true
        //%timefield%: @timestamp
        index: logstash-*
        body: {
          query: {
            match: { program: "bro_conn" }
          },
          size: 0
          aggs: {
            table: {
              composite: {
                size: 1000000
                sources: [
                  { stk1: { terms: {field: "id.orig_h.keyword"} } }
                  { stk2: { terms: {field: "id.resp_h.keyword"} } }
                ]
              }
            }
          }
        }
      }
      // From the result, take just the data we are interested in
      format: {property: "aggregations.table.buckets"}
      // Convert key.stk1 -> stk1 for simpler access below
      transform: [
        {type: "formula", expr: "datum.key.stk1", as: "stk1"}
        {type: "formula", expr: "datum.key.stk2", as: "stk2"}
        {type: "formula", expr: "datum.doc_count", as: "size"}
      ]
    }
    {
      name: nodes
      source: rawData
      transform: [
        // when a country is selected, filter out unrelated data
        {
          type: filter
```

Based on: https://www.elastic.co/blog/sankey-visualization-with-vega-in-kibana

Canvas


kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Guest User
Logout
Privacy Statement
D
Default
Collapse
Refresh
Digital Marketing
Marketing Funnel
120462
Website Visitors
20643
Emails Registered
546
Campaign Responses
123
Conversions
Conversion Ratio
1.03%
Bounce Rate
49.4%
Subscribers by Platform
Youtube
Twitter
Instagram
Facebook
0
24000
Email Campaigns
24
Newsletter Open Rate
53.8%
Campaign Responses
800
600
400
200
0
a: previous year
b: current year
May
Jul
Sep
Nov
Jan
Mar
Weekly Visitors by Day
00:00
04:00
08:00
12:00
16:00
20:00
1: Mon
2: Tue
3: Wed
4: Thu
5: Fri
6: Sat
7: Sun
Finance, Sales, and Marketing
Page 2 of 4

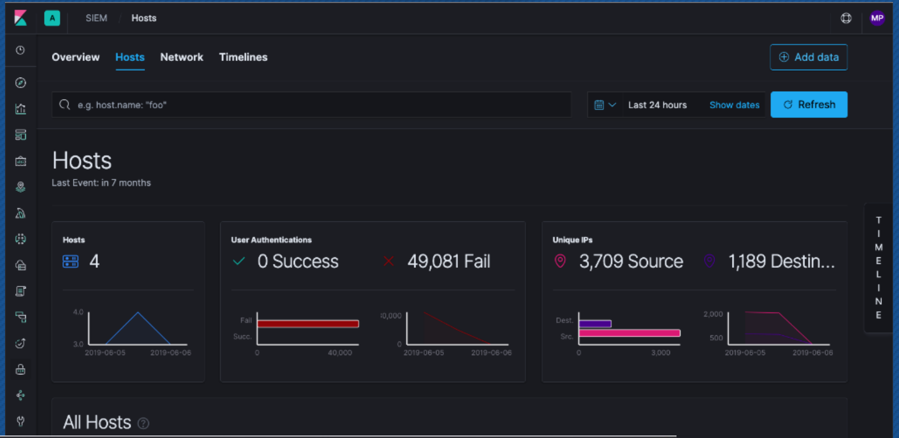
Elastic SIEM



Authentications

Showing: 3,192 Users

User	Failures	Last Failure
root	4040	5 hours ago
admin	1406	5 hours ago
test	1356	5 hours ago
user	524	5 hours ago
guest	400	7 hours ago
123456	334	5 hours ago
oracle	312	5 hours ago
support	270	5 hours ago
tomcat	226	5 hours ago



Hosts

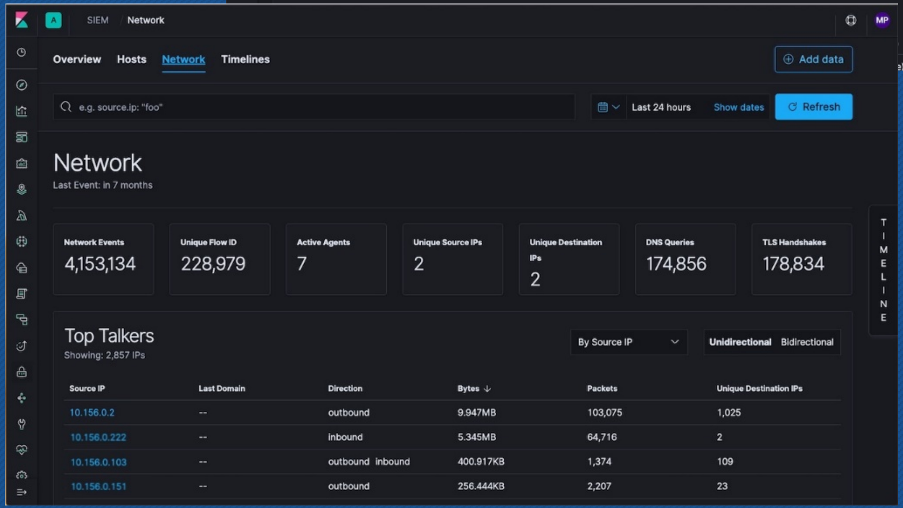
Last Event: in 7 months

Hosts: 4

User Authentications: 0 Success, 49,081 Fail

Unique IPs: 3,709 Source, 1,189 Destin...

All Hosts



Network

Last Event: in 7 months

Network Events	Unique Flow ID	Active Agents	Unique Source IPs	Unique Destination IPs	DNS Queries	TLS Handshakes
4,153,134	228,979	7	2	2	174,856	178,834

Top Talkers

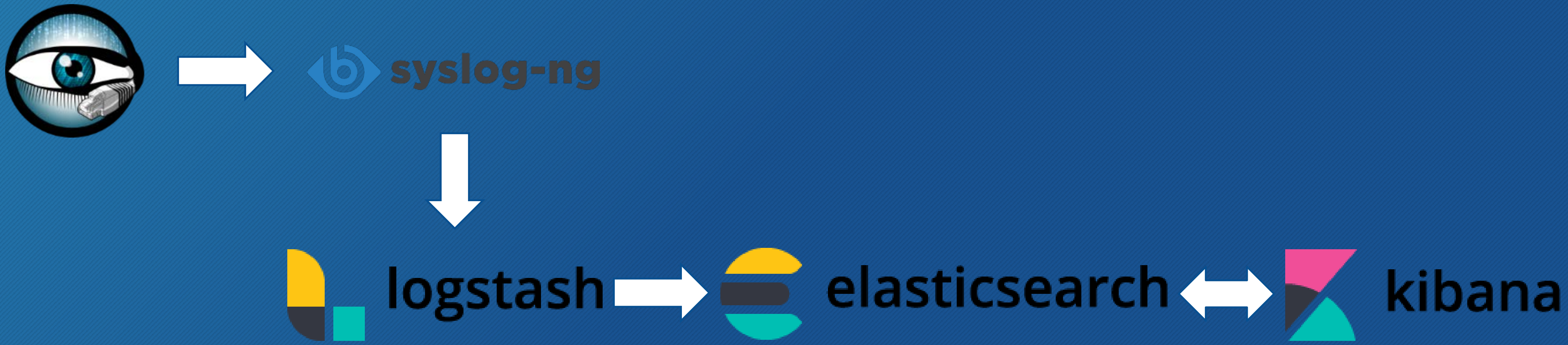
Showing: 2,857 IPs

Source IP	Last Domain	Direction	Bytes ↓	Packets	Unique Destination IPs
10.156.0.2	--	outbound	9.947MB	103,075	1,025
10.156.0.222	--	inbound	5.345MB	64,716	2
10.156.0.103	--	outbound inbound	400.917KB	1,374	109
10.156.0.151	--	outbound	256.444KB	2,207	23

ALZETTE
INFORMATION SECURITY

Source: https://www.elastic.co/blog/introducing-elastic-siem

Kibana Hands-On Scenario



Kibana Hands-On

2019 Pass the SALT Workshop

Elastic Stack Alerting and Security

2019 Pass the SALT Workshop

ALZETTE

INFORMATION SECURITY

Watcher vs. ElastAlert

Watcher

- Part of X-Pack
- https://www.elastic.co/guide/en/x-pack/current/xpack-alerting.html
- Elasticsearch API
- JSON format
- **Watches**: Triggers, Inputs, Conditions, Transforms, Actions

ElastAlert

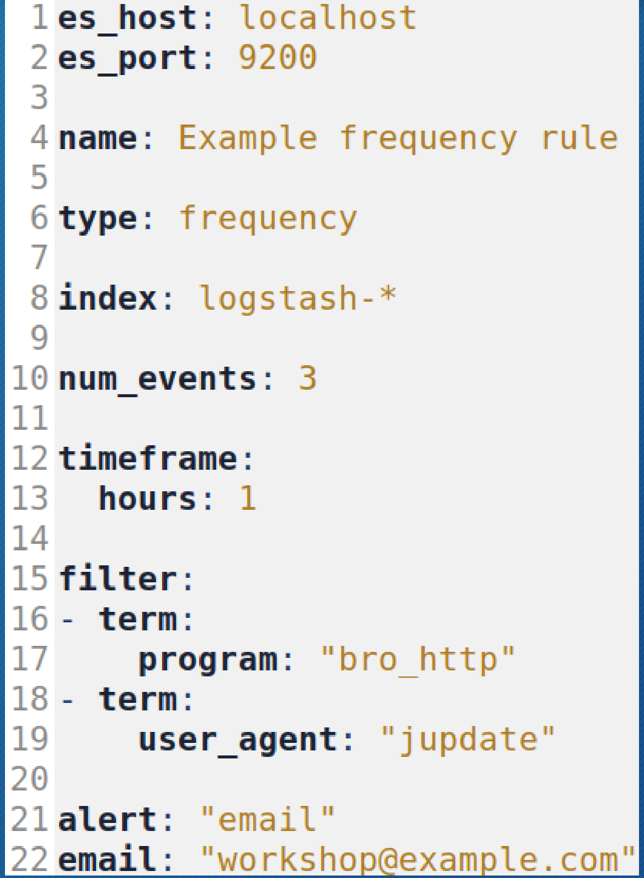
- Developed by Yelp
- https://github.com/Yelp/elastalert
- Simple framework for alerting
- YAML format
- Components: Rules and Alerts

ElastAlert Overview

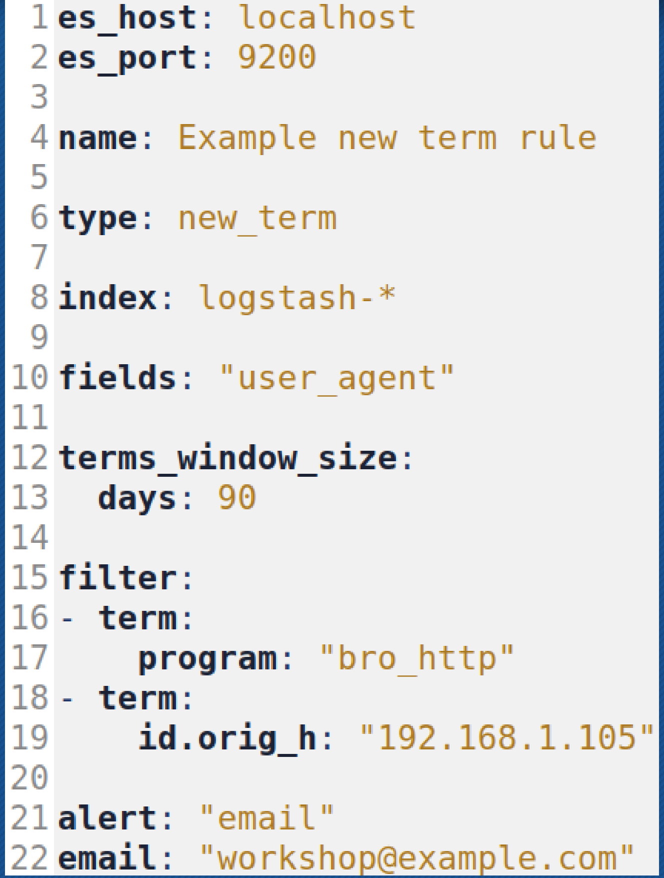
1. Elasticsearch is periodically queried
2. Data is passed to the rules
3. When a match occurs, one or more alerts are triggered
4. Alerts take action based on the match

- **Rule types**: Any, Blacklist, Whitelist, Change, Frequency, Spike, Flatline, New Term, Cardinality, Metric Aggregation, Percentage Match
- **Alert types**: Command, Email, JIRA, ServiceNow, Slack, PagerDuty, GoogleChat, Mattermost, Telegram, etc.
- https://elastalert.readthedocs.io

ElastAlert Examples



```yaml
es_host: localhost
es_port: 9200

name: Example frequency rule

type: frequency

index: logstash-*

num_events: 3

timeframe:
  hours: 1

filter:
- term:
    program: "bro_http"
- term:
    user_agent: "jupdate"

alert: "email"
email: "workshop@example.com"
```



```yaml
es_host: localhost
es_port: 9200

name: Example new term rule

type: new_term

index: logstash-*

fields: "user_agent"

terms_window_size:
  days: 90

filter:
- term:
    program: "bro_http"
- term:
    id.orig_h: "192.168.1.105"

alert: "email"
email: "workshop@example.com"
```

ElastAlert Hands-On

2019 Pass the SALT Workshop

Security

- **Elastic Stack Security**: https://www.elastic.co/products/stack/security
  - Part of **Elastic Stack Features (formerly X-Pack)**
  - “Starting in version 6.8 and 7.1, core security features like TLS, file and native realm authentication, and role-based access control are now free.”
- **ReadonlyREST**: https://readonlyrest.com
  - 3rd party
  - Free community version
- **Search Guard**: https://search-guard.com
  - 3rd party
  - Free community version
- NGINX reverse proxy + Basic Auth: https://www.nginx.com
  - No RBAC at all

Questions and Answers

2019 Pass the SALT Workshop

References

- Elastic Website
  - https://www.elastic.co
- Elastic Documentation
  - https://www.elastic.co/guide/index.html
- John Hubbard - The Elastic Stack as a SIEM
  - https://www.youtube.com/watch?v=v69kyU5XMFI
- ElastAlert
  - https://github.com/Yelp/elastalert