

Detectando e Respondendo Incidentes de Segurança em Frontends Nginx Utilizando ELK

Jerônimo Zucco - jczucco@ucs.br
[@jczucco](https://twitter.com/jczucco)

8º Fórum Brasileiro de CSIRTs - 2019

- Analista GTI/UCS
- Twitter: [@jczucco](https://twitter.com/jczucco)
- <http://www.linkedin.com/in/jeronimozucco>
- Algumas certificações na área de segurança
- https://www.owasp.org/index.php/User:Jeronimo_Zucco
- A apresentação será disponibilizada em <https://www.slideshare.net/jczucco>
- Obs: não represento a Elastic, sou apenas usuário de seus produtos opensource

- Estrutura de rede da UCS
- Rotina de notificação de incidentes
- Centralização de Logs/SIEM
- A pilha ELK
- Construindo Dashboards
- Extrair dados para notificação
- Configurando Nginx
- Funcionalidades na nova versão ELK e assinaturas
- Cuidados na implementação
- Conclusões

- 2 redes IPv4 de 4096 endereços roteáveis cada (8192 IPs)
- AS - Sistema Autônomo
- ~ 5000 computadores na rede interna
- Picos de ~ 12.000 clientes na rede Wireless
- Datacenter próprio
- 2 Links de internet - 3gbits
- Rotas na borda (BGP full routing):
 - 740 mil IPv4
 - 65 mil IPv6

- Firewall de borda de última geração
- Frontends Nginx
- Sites online
 - Sites institucionais
 - AVA (Ambiente Virtual de Aprendizagem)
 - Sistemas Web para diversos fins
 - Sites de projetos acadêmicos

Rotina inicial de notificação de incidentes

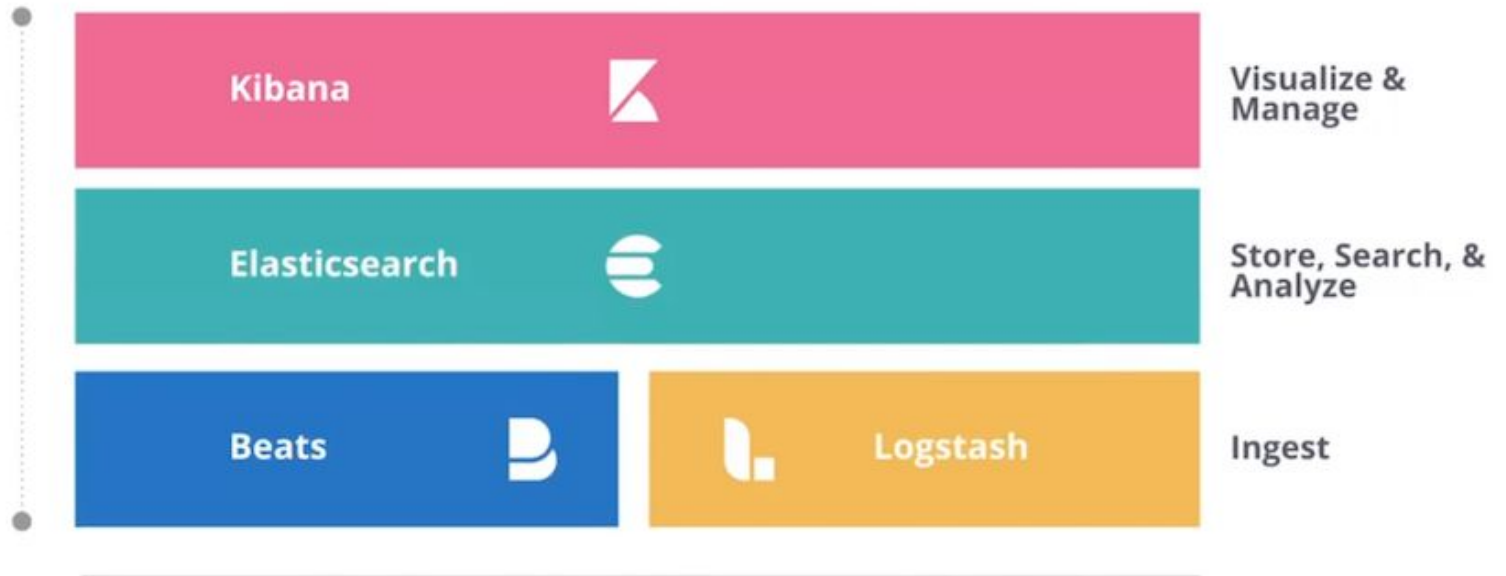
- Logs do Firewall e Frontends
- Pesquisa (grep) por padrões de ataques conhecidos em arquivos de log
 - scans de hacking tools
 - wp-login.php, admin bruteforce
 - SSH bruteforce
 - Directory traversals - /etc/passwd...
 - SQL Injections
 - Erros de aplicação (50x)
 - Monitoramento de acessos indevidos à APIs

- Análise para criação de política de bloqueios
 - badbots
 - evil headers
(nikto|wpscan|openvas|scrapy|sqlmap|Arachni), etc
 - extensões de arquivos de backup/dumps
 - blacklists de urls de ataques conhecidos
- Blacklists/alertas
- SIEM
- Sem verba disponível
- Splunk e ELK

A Pilha ELK

Elastic Stack

SOLUTIONS



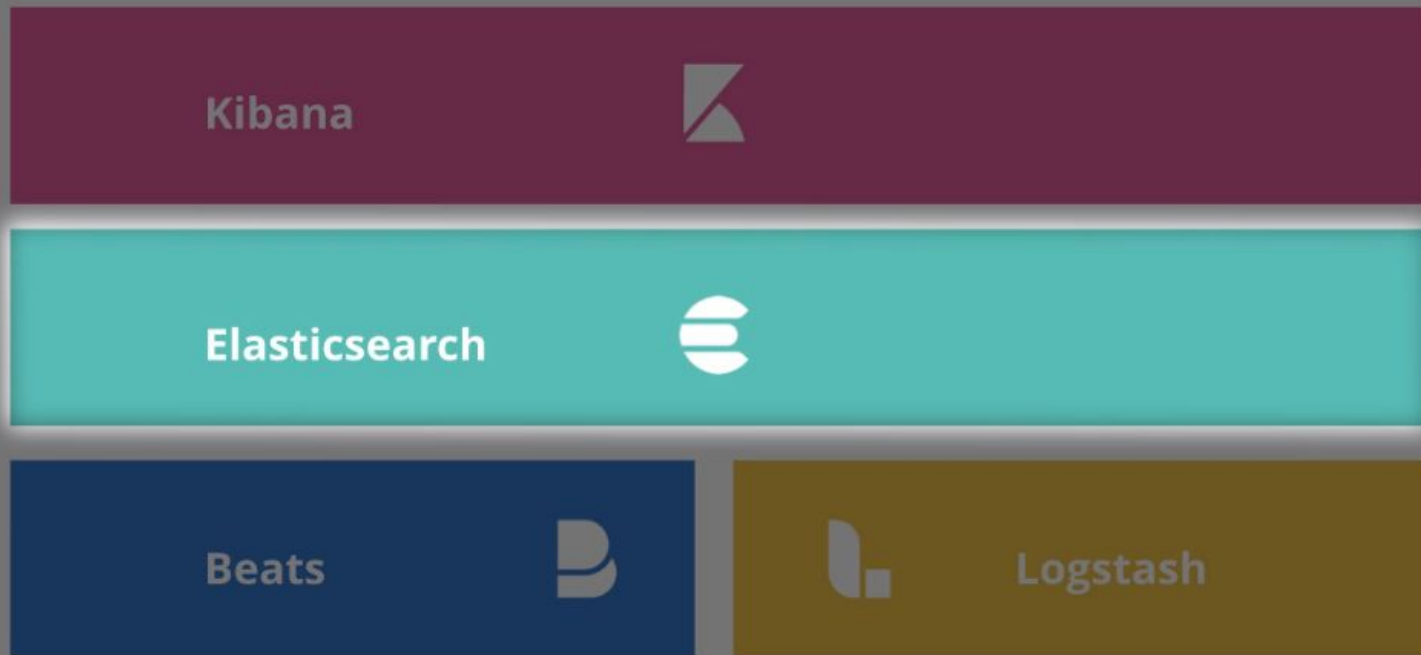
SaaS



SELF-MANAGED



ELASTICSEARCH



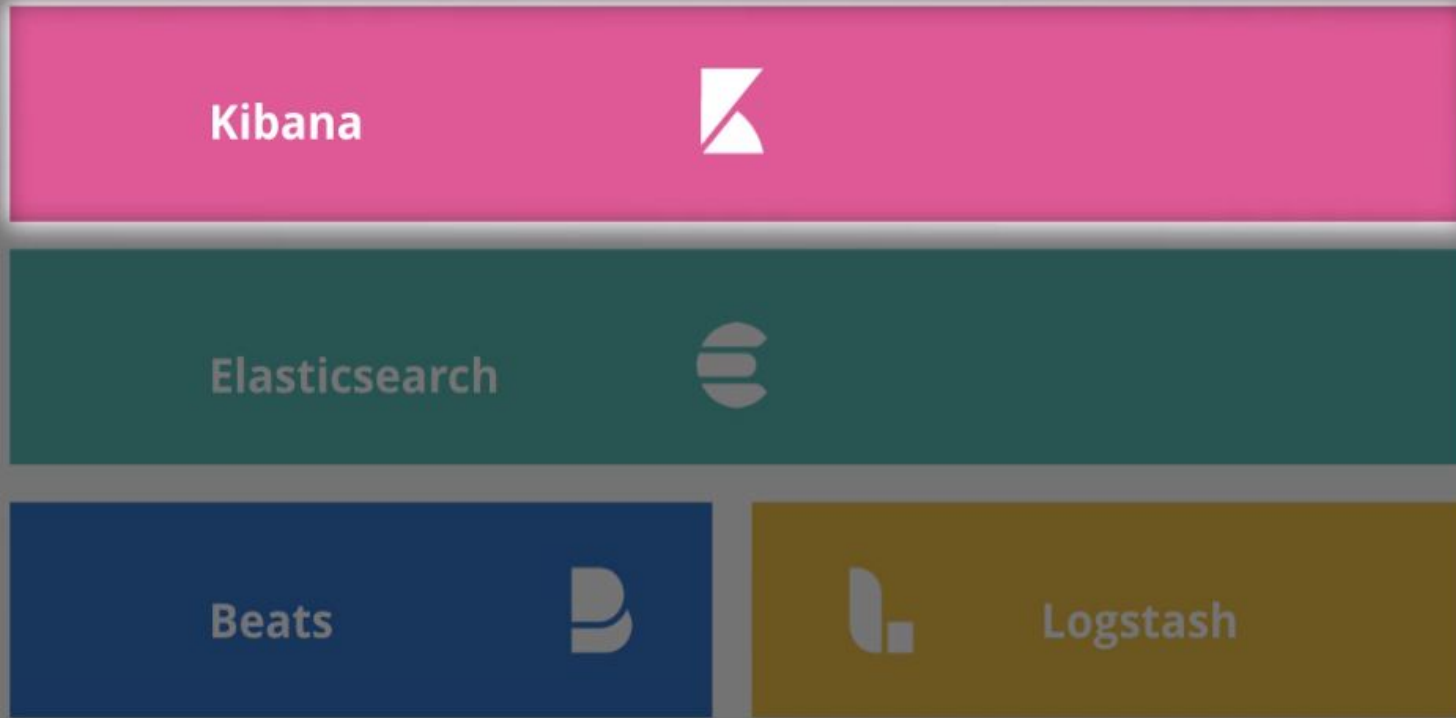
- Parte principal (Core) da pilha ELK
- Base de dados orientada a documentos
- Open Source (Java) <https://github.com/elastic>
- Construído com base no Lucene
- Escalável - cluster e distribuição de carga
- (Near) Armazenamento/busca em tempo real
- muitas consultas por segundo e atualizações dinâmicas dos dashboards
- Alta disponibilidade - tolerante à falhas
- Amigável para desenvolvedores - APIs restful disponíveis
- Armazenamento versátil

- Consultas e agregações, consultas analíticas
- Extensa documentação gratuita disponível
- Cada índice é dividido em *shards*, e cada shard pode ter uma ou mais réplicas
- Disponível on-premise ou na nuvem:
 - <https://cloud.elastic.co/pricing> (a partir de U\$ 16,00, 15 dias trial)
 - Elastic Cloud (SaaS)
 - GCP, AWS ou Azure (recém anunciado)

KIBANA



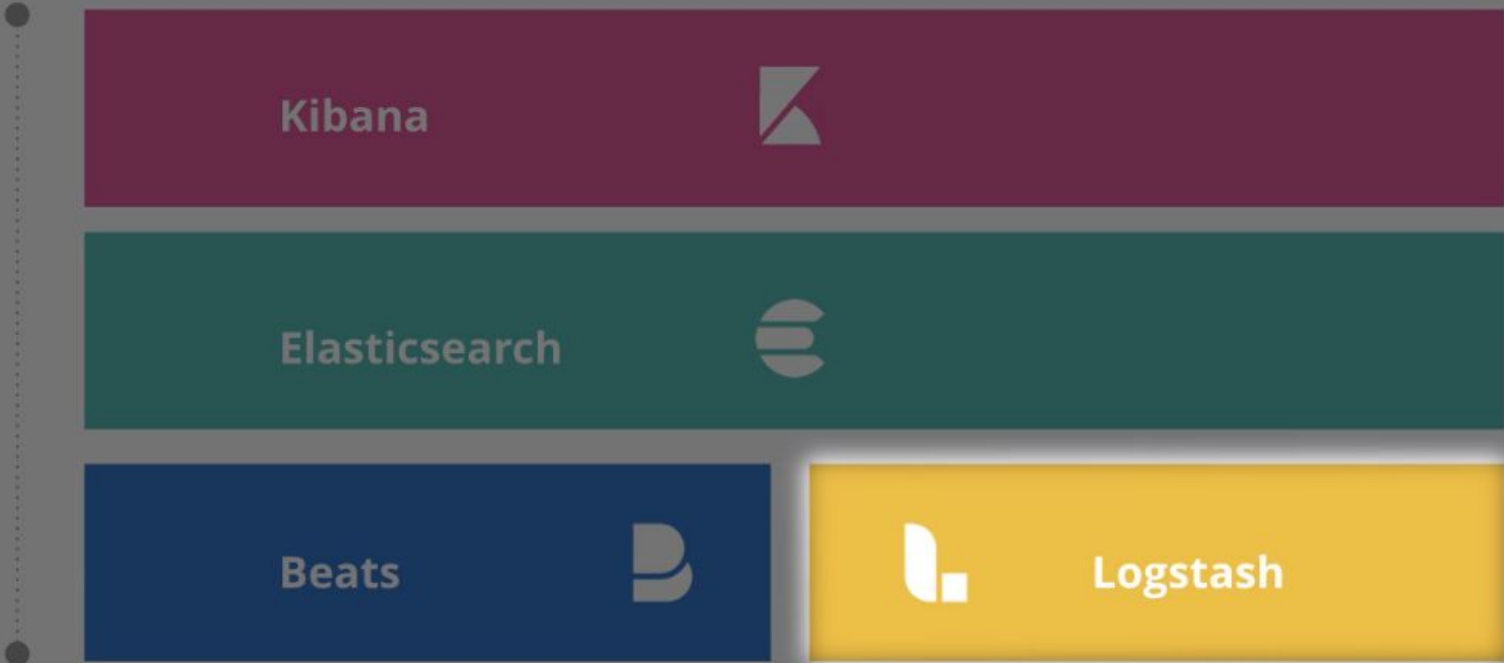
Elastic Stack



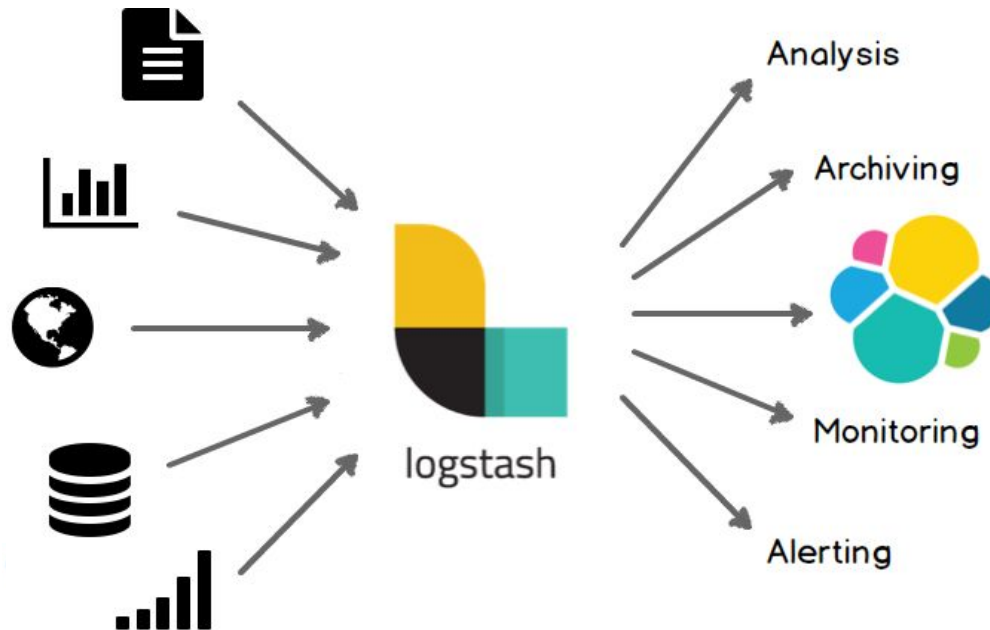
- Ferramenta analítica
- Interface Web para pesquisa e visualização (consultas e filtros)
- Agregações complexas, gráficos e tabelas
- Frequentemente utilizado para análise de LOGs (adeus grep!)
- Interação com os índices e exploração sem escrita de código
- Trabalha com dados em tempo real
- Gerência centralizada do Elasticsearch
- Criação de Dashboards e Canvas

LOGSTASH

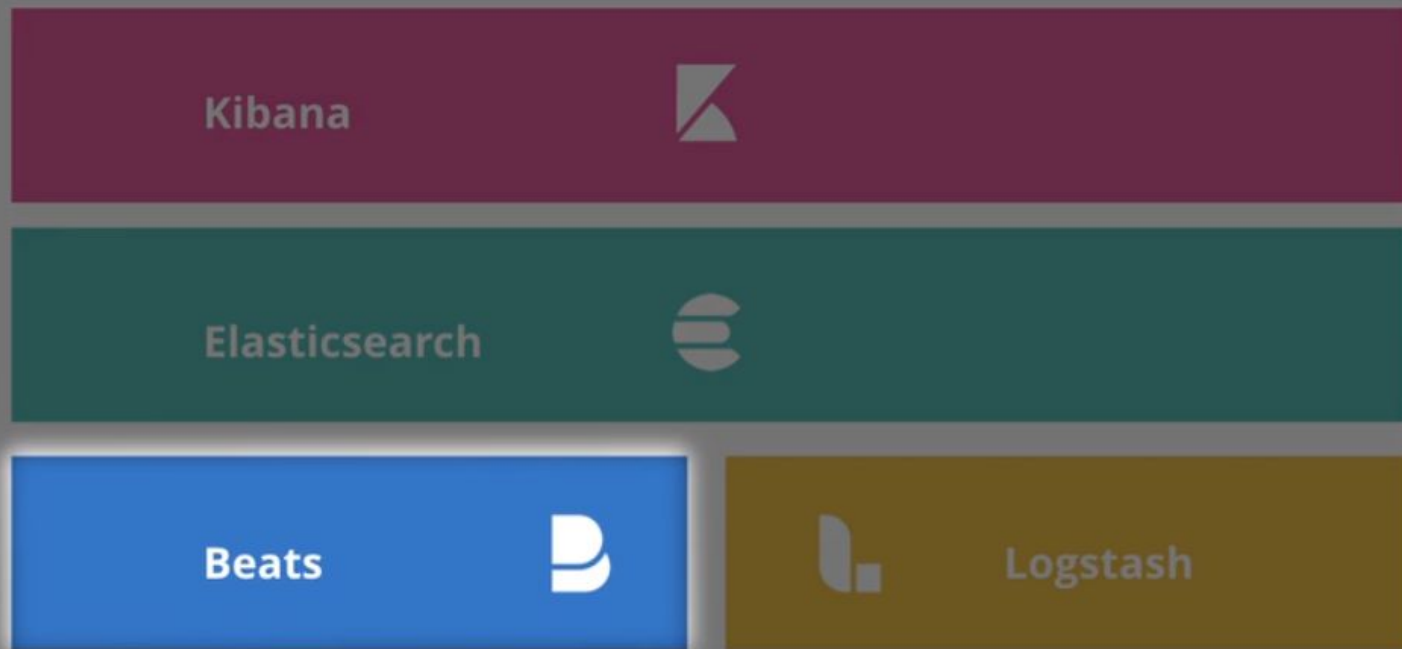
Elastic Stack



- Escrito em JRuby (roda na JVM)
- Opcional para tratar/enriquecer a informação antes de enviar para o elasticsearch (pipeline ETL)
- Grok filters, plugins com formatos padrões
- Buffer para envio de dados



BEATS



Logging modules

AUDITBEAT

FILEBEAT

WINLOGBEAT



Infrastructure

System

- Linux / MacOS
- Windows Events

Containers

- Docker
- Kubernetes

Applications

Databases

- MySQL
- PostgreSQL

Queues

- Kafka
- Redis

Web servers

- Apache
- Nginx

Audit data

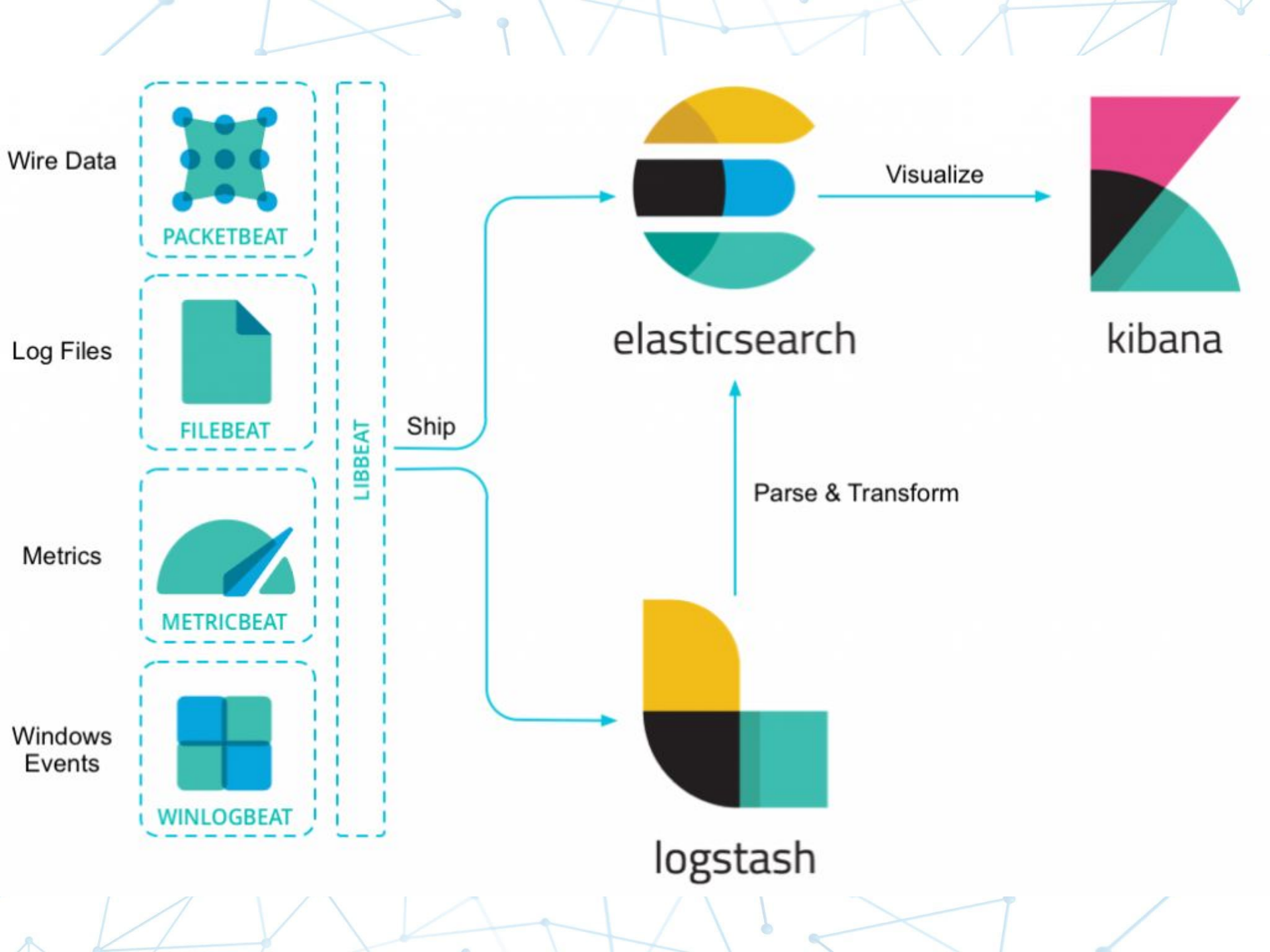
- Filesystem
- System calls

- protocolo para não sobrecarregar a origem dos logs, o logstash e o elasticsearch
- mantém controle do ponto de leitura dos arquivos de logs

logs -> filebeat -> logstash (opcional) -> elasticsearch -> kibana

```
# filebeat modules list
```

```
# filebeat modules enable nginx
```



Wire Data



PACKETBEAT

Log Files



FILEBEAT

Metrics



METRICBEAT

Windows Events



WINLOGBEAT

LIBBEAT

Ship



elasticsearch

Visualize



kibana

Parse & Transform










logstash

- Antes de instalar: número de nodos, réplicas, tipo de uso, estimativa de recursos
- Uso inicial de testes na UCS (versão 5)
- Centralização de Logs de servidores/serviços (DHCP, DNS, impressão, autenticação, winlog, etc)
- Depois com mais recursos, adicionados logs dos servidores nginx (grande quantidade de logs)
- Processos de upgrades

Criando Dashboards no Kibana













- Criar e salvar a pesquisa
- Criar os diversos gráficos de visualização vinculado à pesquisa salva
- Criar a dashboard agrupando os gráficos
- Criar novas pesquisa e copiar os gráficos associando à essa nova pesquisa através da edição de objetos no Kibana

 **kibana**

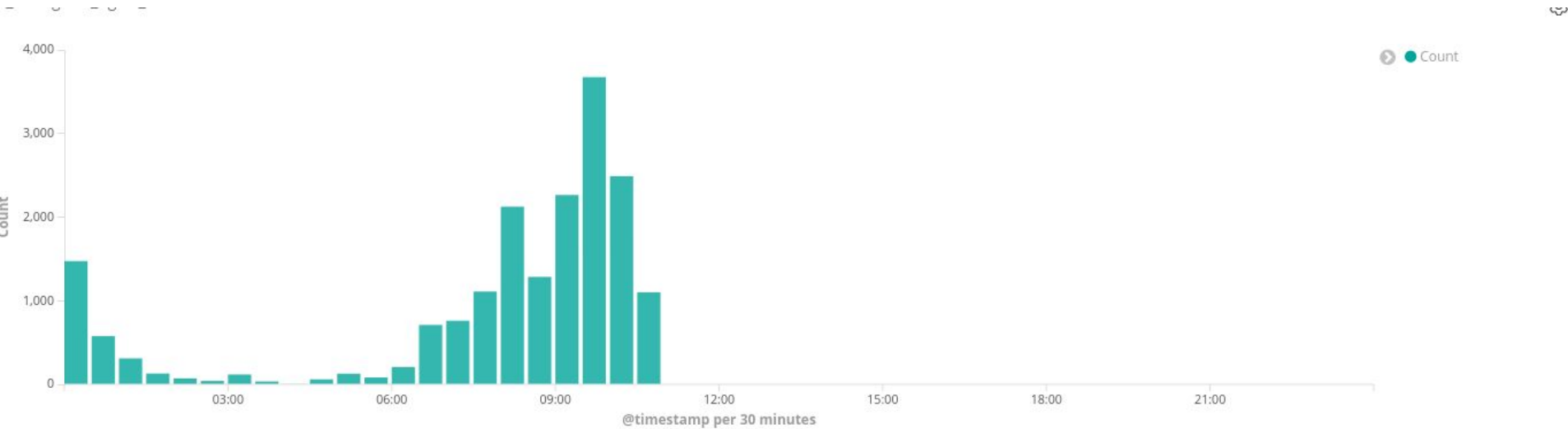
-  Discover
-  **Visualize**
-  Dashboard
-  Timelion
-  Canvas
-  Maps
-  Machine Learning
-  Infrastructure
-  Logs
-  APM
-  Uptime
-  Dev Tools
-  Monitoring

Visualize

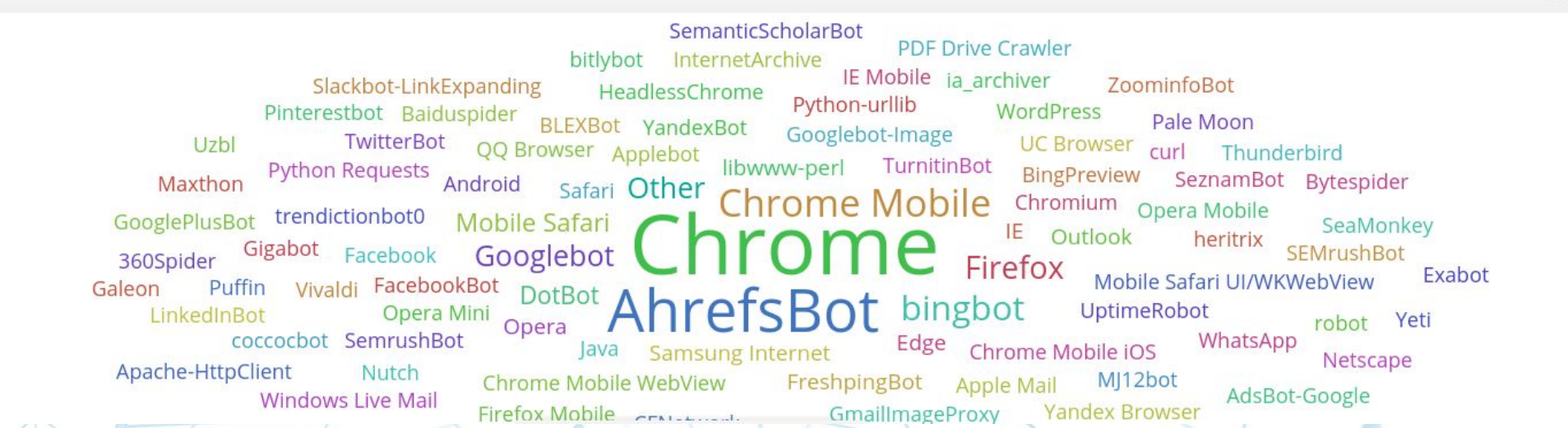
+

<input type="checkbox"/> Title ↑	Type
<input type="checkbox"/> V_Dispositivo_Search_nginx_API	 Pie
<input type="checkbox"/> V_Dispositivo_Search_nginx_WWW	 Pie
<input type="checkbox"/> V_IP_Search_nginx_API	 Data Table
<input type="checkbox"/> V_IP_Search_nginx_WWW	 Data Table
<input type="checkbox"/> V_Map_Search_nginx_API	 Coordinate Map
<input type="checkbox"/> V_Map_Search_nginx_WWW	 Coordinate Map
<input type="checkbox"/> V_OS_Search_nginx_API	 Tag Cloud
<input type="checkbox"/> V_OS_Search_nginx_WWW	 Tag Cloud
<input type="checkbox"/> V_Response_code_Search_nginx_API	 Pie
<input type="checkbox"/> V_Response_code_Search_nginx_WWW	 Pie
<input type="checkbox"/> V_URLS_Search_nginx_API	 Data Table
<input type="checkbox"/> V_URLS_Search_nginx_WWW	 Data Table

Acessos por User-agent



_UserAgent_WWW



Acessos por Geolocalização

Visualize / V_Map_Search_nginx_API.png

Save Share Inspect Refresh Documentation Auto-refresh This week

Linked to Saved Search Search_nginx_API

> Search... (e.g. status:200 AND extension:PHP) Options Refresh

Add a filter +

filebeat-*

Data Options

Metrics

- Value Count

Buckets

- Geo Coordinates

Aggregation [Geohash help](#)

Geohash

Field

nginx.access.geolp.location

- Change precision on map zoom
- Place markers off grid (use geocentroid)
- Only request data around map extent

Custom Label

Advanced

Map visualization showing cities and markers across South America (Colombia, Ecuador, Peru, Bolivia, Paraguay, Chile, Argentina, Brazil, Uruguay, Suriname).

Count legend:

- 1 - 3,706.75
- 3,706.75 - 7,412.5
- 7,412.5 - 11,118.25
- 11,118.25 - 14,824

© OpenStreetMap contributors, OpenMapTiles, MapTiler, Elastic Maps Service

Acessos por HTTP Response

Visualize / V_Response_code_Search_nginx_API

Save Share Inspect Refresh Documentation Auto-refresh Last 15 minutes

Linked to Saved Search Search_nginx_API

Search... (e.g. status:200 AND extension:PHP) Options Refresh

Add a filter +

filebeat-*

Data Options

Metrics

Slice Size Count

Buckets

Split Slices

Aggregation Terms

Field nginx.access.response_code

Order By metric: Count

Order Descend Size 10

Group other values in separate bucket

Show missing values

Custom Label Response Code

Response Code	Count
200	~95
201	~2
301	~2
404	~1
499	~1

Dashboard - Acessos à API

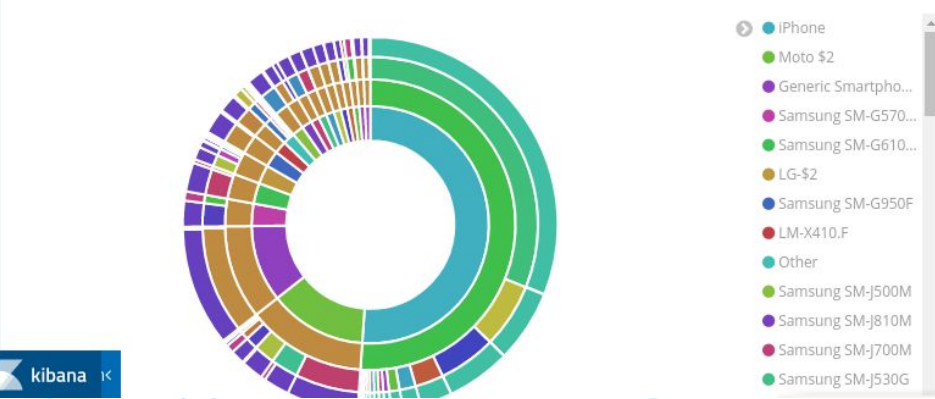
V_Map_Search_nginx_API.png



V_Response_code_Search_nginx_API



V_Dispositivo_Search_nginx_API



V_OS_Search_nginx_API



Dashboard - Acessos à API



- iPhone
- Moto \$2
- Generic Smartpho...
- Samsung SM-G570...
- Samsung SM-G610...
- LG-\$2
- Samsung SM-G950F
- LM-X410.F
- Other
- Samsung SM-J500M
- Samsung SM-J810M
- Samsung SM-J700M
- Samsung SM-J530G
- Samsung SM-G9650
- Samsung SM-G9600



Count - nginx.access.user_agent.os: Descending

V_URLS_Search_nginx_API

URL	Count
	2,363
	2,356
	2,318
	2,246
	2,241
	2,158
	2,155
	1,817
	310
	277

V_IP_Search_nginx_API

IP	Count
10.70.10.74	256
177.10.111.139	221
10.20.30.234	214
138.36.81.238	166
10.70.1.223	165
10.20.21.97	160
2804:18:32:dffc:6016:13cc:b73e:39f6	159
201.139.95.5	155
10.20.15.202	148
10.20.28.134	147

Monitorando acessos via Kibana e realizando notificação de incidente

Identificando um Ataque

V_Map_Search_nginx_WWW



V_Response_code_Search_nginx_WWW



V_Dispositivo_Search_nginx_WWW



V_OS_Search_nginx_WWW

Other
Ubuntu Linux
Windows 10

Identificando um Ataque



- Other
- Ubuntu
- Windows 10
- Linux
- Firefox
- Edge
- Chrome

Other
Ubuntu Linux
Windows 10

Count - nginx.access.user_agent.os: Descending

V_URLS_Search_nginx_WWW

URL	Count
/	64
/index.php	22
/login.php	19
/index.pl	18
/cgi-bin/authLogin.cgi	17
/login.pl	17
/cgi-bin/env.cgi	16
/cgi-bin/environment.cgi	16
/cgi-bin/index.cgi	16
/cgi-bin/f.cgi	16

V_IP_Search_nginx_WWW

IP	Count
174.128.225.10	6,045

Filter for value

Extraindo logs do Elasticsearch

```
curl -H 'Content-Type: application/json' -XGET '127.0.0.1:9200/filebeat-*/_search?pretty' -d '{
```

```
  "query": {
```

```
    "match": {
```

```
      "nginx.access.remote_ip": {
```

```
        "query": "174.128.225.10"
```

```
      }
```

```
    }
```

```
  }, "size": 100
```

```
}'
```

Código [getlogip.py](#)

```
import sys,ipaddress
from elasticsearch import Elasticsearch
client = Elasticsearch()

try:
    IP = ipaddress.ip_address(sys.argv[1])
    IP=sys.argv[1]
except ValueError:
    print('IP address invalid: %s' % sys.argv[1])
    sys.exit(2)
except:
    print('Usage : %s <IP ADDRESS>' % sys.argv[0])
    sys.exit(2)

response = client.search(
    index="filebeat-*",
    body={
        "query": {
            "match": {
                "nginx.access.remote_ip": {
                    "query": IP
                }
            }
        }, "size": 100
    }
)

for hit in response['hits']['hits']:
    print("%s" | "%s" | "%s" | "%s" | "%s" % (
        hit['_source']['@timestamp'],
        hit['_source']['nginx']['access']['remote_ip'],
        hit['_source']['nginx']['access']['method'],
        hit['_source']['nginx']['access']['url'],
        hit['_source']['nginx']['access']['user_agent']['original']
    ))
```


Configurando o Frontend Nginx

```
map $http_user_agent $bad_bot {
    default 0;
    ~*^Lynx 0; # Let Lynx go through
    ~*(?i)(httrack|htmlparser|JikeSpider|proximic|Sosospider|Baiduspider|msnbot|rawl
er|Baiduspider|Siteimprove|Aboundex|80legs|360Spider|^Java|Cogentbot|^Alexible|^Blac
kWidow|^BlowFish|^BotALot|Buddy|^BuiltBotTough|^Bullseye|^BunnySlippers|k|^cosmos|^C
rescent|^Custo|^AIBOT|ZmEu|MJ12bot|MegaIndex|OpenLinkProfiler|spbot|ition\Campaign|
AhrefsBot|QQBrowser) 1;urnitinBot|Scrapy|OpenVAS|SemrushBot|Edd
}

if ($bad_bot) { return 403; }
```

Bloqueios por URL

```
location ~ /\.ht {  
    deny all;  
}  
location ~ wp-login.php {  
    deny all;  
}  
location ~ /etc/passwd {  
    deny all;  
}  
location ~* /\.svn {  
    deny all;  
}  
location ~* /\.git {  
    deny all;  
}
```

```
proxy_intercept_errors on;
```

```
error_page 500 502 503 504 /erro/50x.html;
```

```
limit_req_zone $binary_remote_addr zone=mylimit:10m rate=10r/s;
```

```
server {
```

```
    location /login/ {
```

```
        limit_req zone=mylimit;
```

```
        proxy_pass http://my_upstream;
```

```
    }
```

```
}
```

Opções de Subscrição

GRATUÍTO

SUBSCRIÇÃO

OPEN SOURCE

BASIC

GOLD

PLATINUM

ENTERPRISE

Open Source
Features

Free Proprietary
Features

Paid Proprietary
Features

Elastic Support

Elastic Cloud
Enterprise

Elastic Support

SELF-MANAGED

SUBSCRIÇÃO

ELASTIC CLOUD

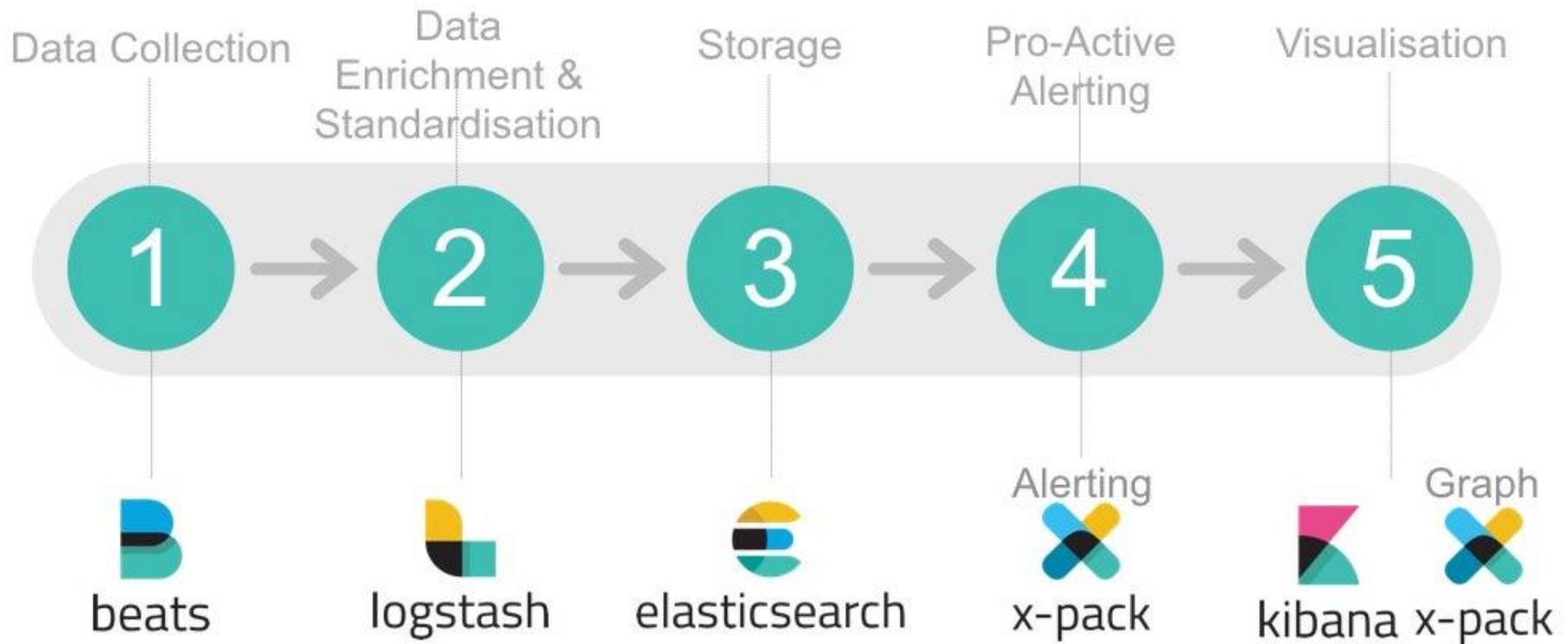
Elasticsearch Service

Elastic App Search Service

Elastic Site Search Service

SaaS

Security and Threat Detection with the Elastic Stack



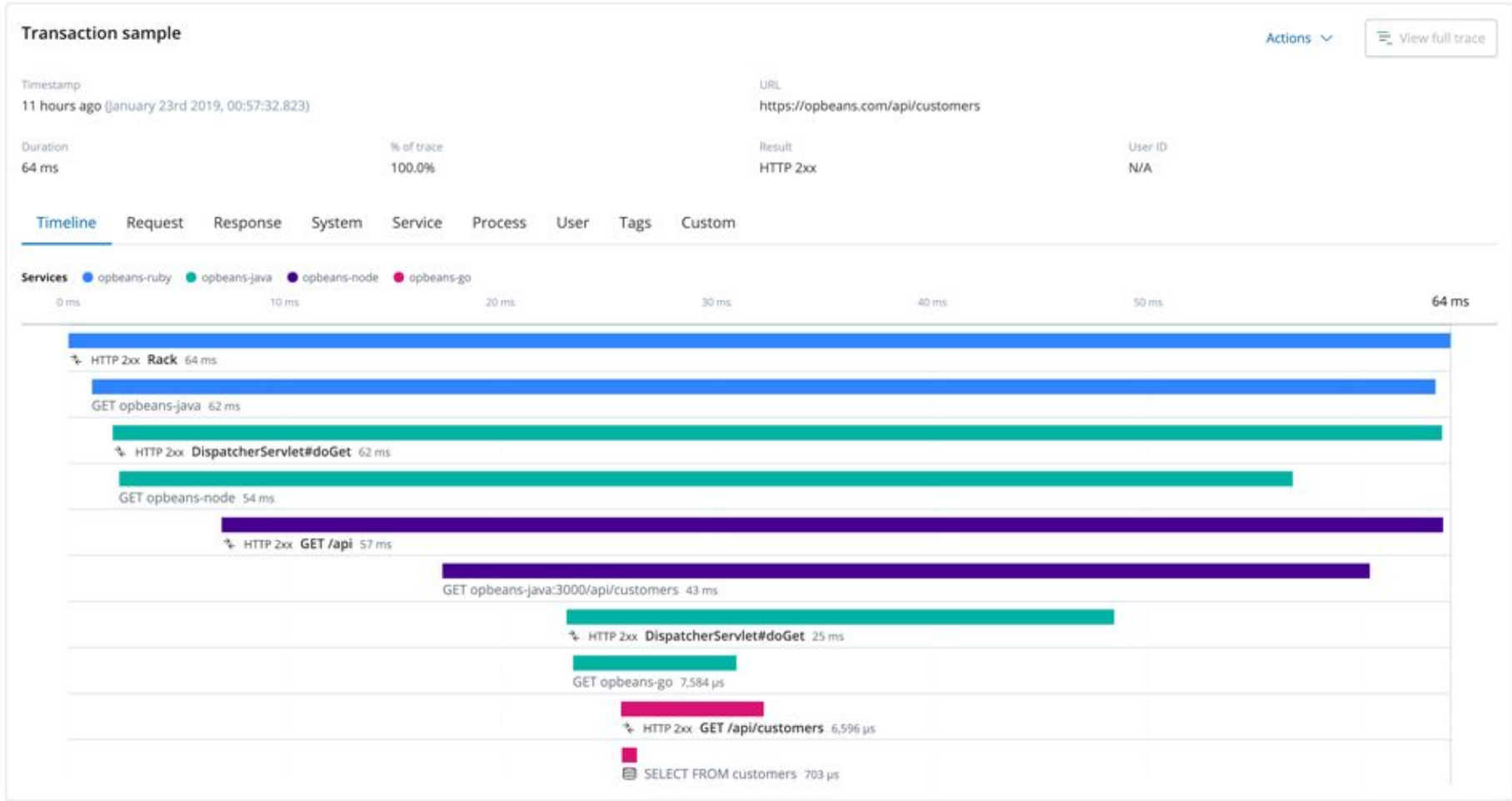
- Extensão do elasticsearch
- De código aberto, porém exige licença para uso
- Na versão 7.x o X-Pack já vem pré-instalado, porém somente algumas funções são gratuitas
 - basic monitoring health
 - basic security
- Funções pagas:
 - alerting
 - security
 - machine learning (beta free do Data Visualizer com upload de arquivo até 100MB)

Subscriptions

Free X-Pack features included in Basic

Elastic Support included in Gold, Platinum, and Enterprise Subscriptions

	OPEN SOURCE	BASIC	GOLD	PLATINUM	ENTERPRISE
	Free Download	Free License	Request Info	Request Info	Request Info
THE ELASTIC STACK					
Elasticsearch	✓	✓	✓	✓	✓
Kibana	✓	✓	✓	✓	✓
Beats	✓	✓	✓	✓	✓
Logstash	✓	✓	✓	✓	✓
APM - agents and server	✓	✓	✓	✓	✓
X-PACK					
✓ Security (formerly Shield)			✓	✓	✓
✓ Monitoring (formerly Marvel)		✓	✓	✓	✓
✓ Management		✓	✓	✓	✓
✓ Alerting (via Watcher)			✓	✓	✓
✓ Machine Learning				✓	
✓ APM		✓	✓	✓	✓
✓ Graph Analytics & Visualization				✓	✓
✓ Reporting		✓	✓	✓	✓
✓ Modules		✓	✓	✓	✓
✓ Dev Tools		✓	✓	✓	✓



E. ALERT DASHBOARD

-- ANY --

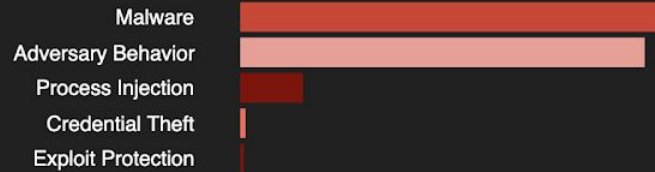
Last 7 days



266
Threats

218
Adversary Behaviors

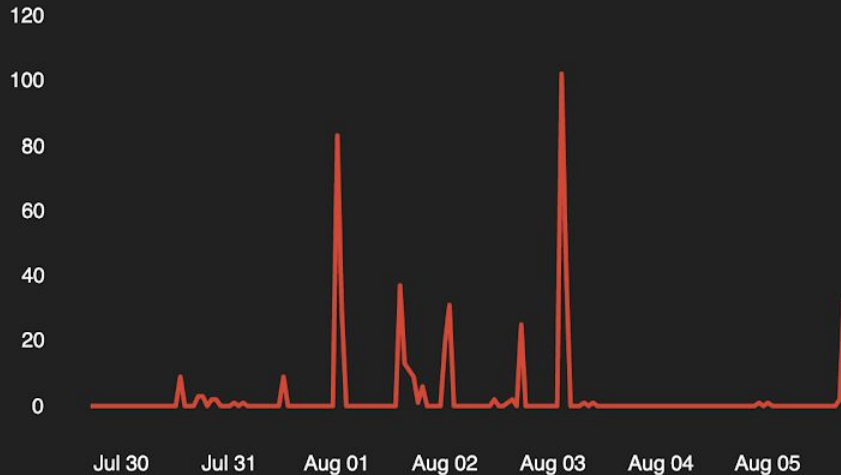
ALERTS BY TYPE



TOP ALERT TYPES

Malware	230
Adversary Behavior	218
Process Injection	33
Credential Theft	2
Exploit Protection	1

ALERTS OVER TIME

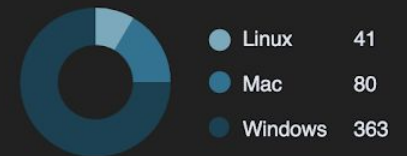


ALERT BREAKDOWN

29
Preventions

455
Detections

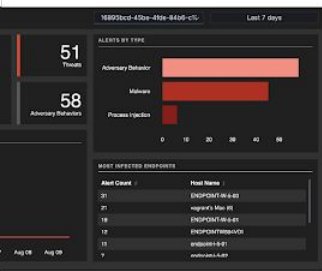
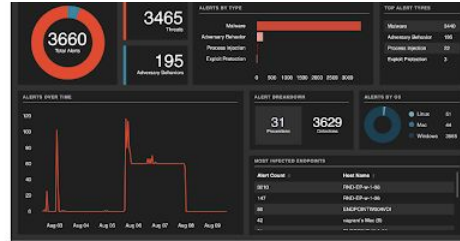
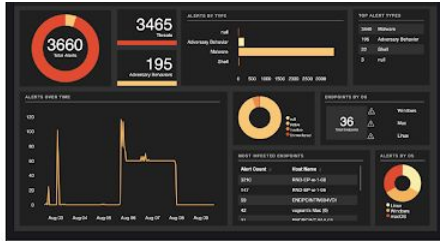
ALERTS BY OS



MOST INFECTED ENDPOINTS

Alert Count #	Host Name
83	ENDPOINT-W-5-03
58	ENDPOINT-W-5-01
43	vagrant's Mac (37)
42	ENDPOINTW504VDI

Canvas - Endgame



SIEM / Hosts

Overview Hosts Network Timelines ⊕ Add data

🔍 e.g. host.name: "foo" 📅 Last 4 hours Show dates 🔄 Refresh

Hosts

Last Event: in 13 days

Hosts

📄 123

User Authentications

✓ 10 Success ✗ 2,495 Fail

Unique IPs

📍 326 Source 📍 408 Desti...

All Hosts

Showing: 123 Hosts

Name	Last Seen ↓	OS	Version
raspberrypi	Jun 11, 2019 @ 16:23:55.612	Raspbian GNU/Linux	9 (stretch)
siem-windows	Jun 11, 2019 @ 16:23:55.545	Windows Server 2019 Datacenter	10.0
suricata-iowa	Jun 11, 2019 @ 16:23:55.091	Ubuntu	18.04.2 LTS (Bionic Beaver)
beats-ci-immutable-ubuntu-1604-1560283326623155464	Jun 11, 2019 @ 16:23:53.981	Ubuntu	16.04.6 LTS (Xenial Xerus)
beats-ci-immutable-centos-7-1560277886160227994	Jun 11, 2019 @ 16:23:53.459	CentOS Linux	7 (Core)
zeek-iowa	Jun 11, 2019 @ 16:23:52.930	Ubuntu	18.04.2 LTS (Bionic Beaver)
beats-ci-immutable-ubuntu-1604-1560282003319232752	Jun 11, 2019 @ 16:23:52.764	Ubuntu	16.04.6 LTS (Xenial Xerus)
siem-es	Jun 11, 2019 @ 16:23:48.754	Debian GNU/Linux	9 (stretch)
beats-ci-immutable-centos-7-1560283326623338348	Jun 11, 2019 @ 16:23:47.260	CentOS Linux	7 (Core)

SIEM / Network

Overview Hosts Network Timelines ⊕ Add data

🔍 not destination.ip:10.0.0.0/8 📅 Last 4 hours Show dates 🔄 Refresh

Network

Last Event: in 13 days

Network Events

305,680

DNS Queries

175

Unique Private IPs

📍 115 Source 📍 0 Destination

Unique Flow IDs

1,755

TLS Handshakes

578

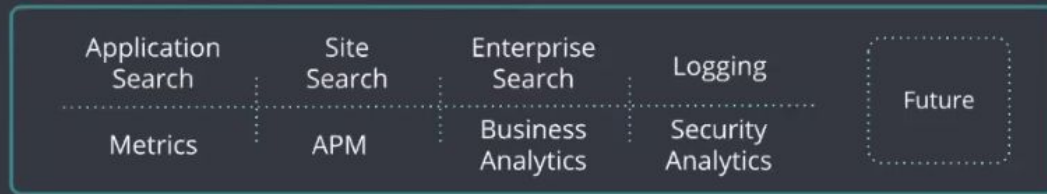
Top Talkers

Showing: 27 IPs By Destination IP Unidirectional Bidirectional

Destination IP	Last Domain	Direction	Bytes ↓	Packets	Unique Source IPs
35.227.125.33	---	---	730.375GB	1,569,101,917	2
151.101.186.217	---	outbound	38.819MB	1,808	2
34.194.52.159	api.smartthings.com	outbound	2.454MB	30,959	2
35.202.116.96	us-central1-gce.archive.ubu-rtu.com	outbound	454.263KB	98	1
35.225.153.130	us-central1-gce.archive.ubu-rtu.com	outbound	434.469KB	67	1

T
I
M
E
L
I
N
E

Elastic Stack - Deploy



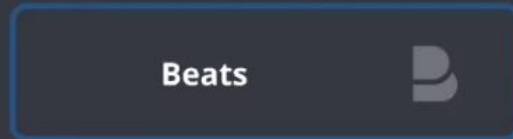
Solutions



Visualize & Manage



Store, Search, & Analyze



Ingest



Deployment



Elastic Stack

Elastic Stack - Subscriptions

OPEN SOURCE

Security

- Encrypted communications
- Role-based access control
- File and native authentication
- Kibana Spaces
- Kibana feature control
- Audit logging
- IP filtering
- LDAP, PKI*, Active Directory authentication
- Elasticsearch Token Service
- Single sign-on (SAML, OpenID Connect, Kerberos*)
- Attribute-based access control
- Field- and document-level security
- Custom authentication & authorization realms
- Encryption at rest support
- FIPS 140-2 mode

BASIC

Security

- Encrypted communications
- Role-based access control
- File and native authentication
- Kibana Spaces
- Kibana feature control
- Audit logging
- IP filtering
- LDAP, PKI*, Active Directory authentication
- Elasticsearch Token Service
- Single sign-on (SAML, OpenID Connect, Kerberos*)
- Attribute-based access control
- Field- and document-level security
- Custom authentication & authorization realms
- Encryption at rest support
- FIPS 140-2 mode

GOLD

Security

- Encrypted communications
- Role-based access control
- File and native authentication
- Kibana Spaces
- Kibana feature control
- Audit logging
- IP filtering
- LDAP, PKI*, Active Directory authentication
- Elasticsearch Token Service
- Single sign-on (SAML, OpenID Connect, Kerberos*)
- Attribute-based access control
- Field- and document-level security
- Custom authentication & authorization realms
- Encryption at rest support
- FIPS 140-2 mode

PLATINUM

Security

- Encrypted communications
- Role-based access control
- File and native authentication
- Kibana Spaces
- Kibana feature control
- Audit logging
- IP filtering
- LDAP, PKI*, Active Directory authentication
- Elasticsearch Token Service
- Single sign-on (SAML, OpenID Connect, Kerberos*)
- Attribute-based access control
- Field- and document-level security
- Custom authentication & authorization realms
- Encryption at rest support
- FIPS 140-2 mode

Vazamentos de Bases Elasticsearch

- [Novembro/2018](#) - 57 milhões de cidadãos americanos expostos encontrados por um scan via Shodan
- [Maiio/2019](#) - PathEvolution
- [Julho/2019](#) - Vazamento de dados dos cidadãos Chilenos
- [Agosto/2019](#) - Honda Motors Company databases leaked 40GB of employee data

[Shodan report:](#) 26,000 Kibana instances that are currently exposed on the Internet

- [Webinars disponibilizados pela Elastic](#)
- [Elasticsearch - The Definitive Guide](#)
- [Canal da Elastic no Youtube](#)
- [ElastiCon Tour SP -](#)
- [Getting Started With Kibana Advanced Searches](#)

- cert.br e organização do fórum
- UCS
- Aos colegas da UCS Marcelo Zorzi e Maurício Gardini

Obrigado

jczucco@ucs.br - [@jczucco](#)

Apresentação será disponibilizada em <https://www.slideshare.net/jczucco>