UCS
UNIVERSIDADE
DE CAXIAS DO SUL

Detectando e Respondendo Incidentes de Segurança em Frontends Nginx Utilizando ELK

Jerônimo Zucco - jczucco@ucs.br
@jczucco

8º Fórum Brasileiro de CSIRTs - 2019

FUNDAÇÃO UNIVERSIDADE
DE CAXIAS DO SUL

Sobre mim

- Analista GTI/UCS
- Twitter: @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

Agenda

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

Estrutura de Rede da UCS

- 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

Estrutura de Rede da UCS

- 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

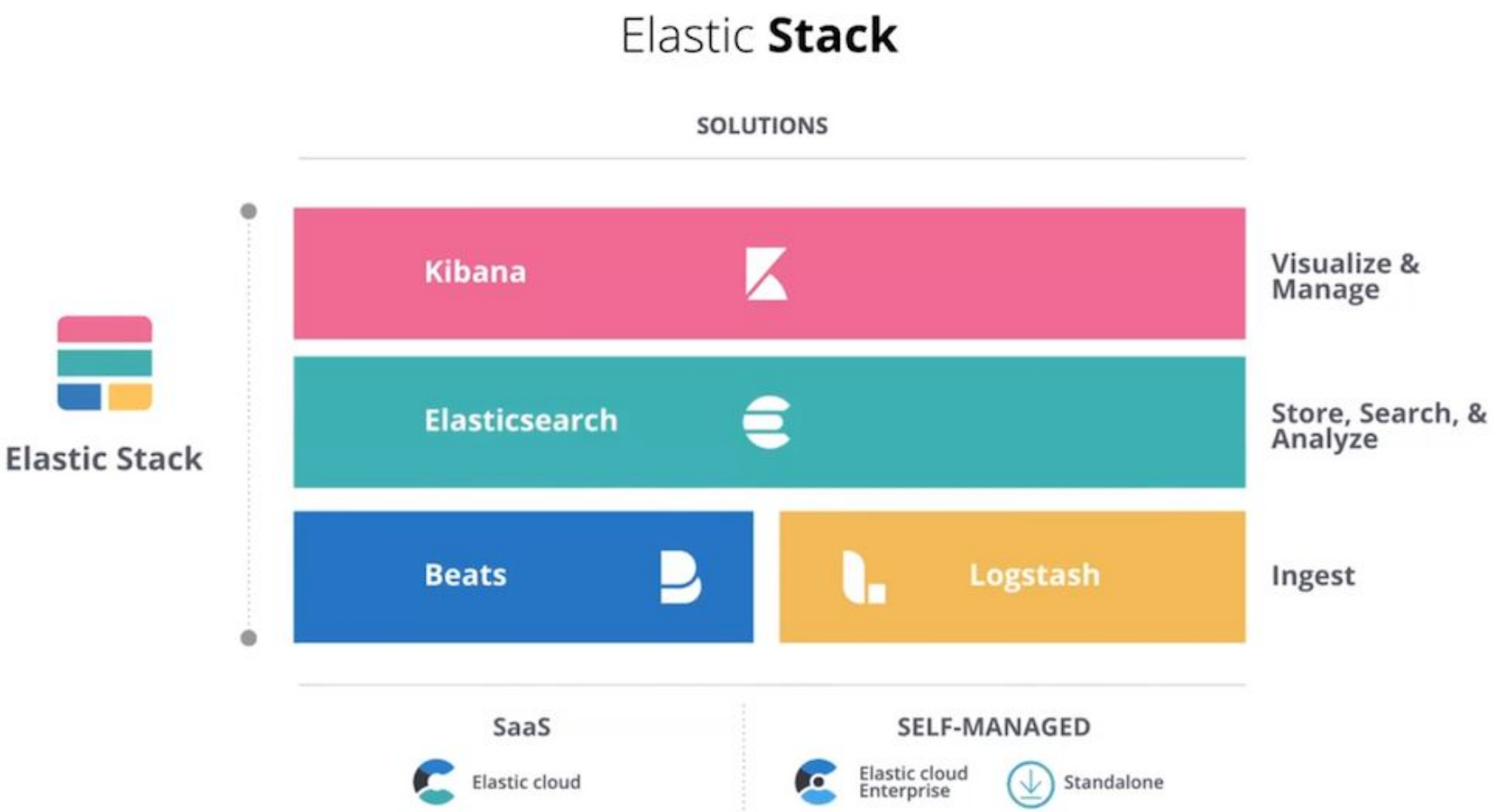
Rotina inicial de notificação de incidentes

- 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

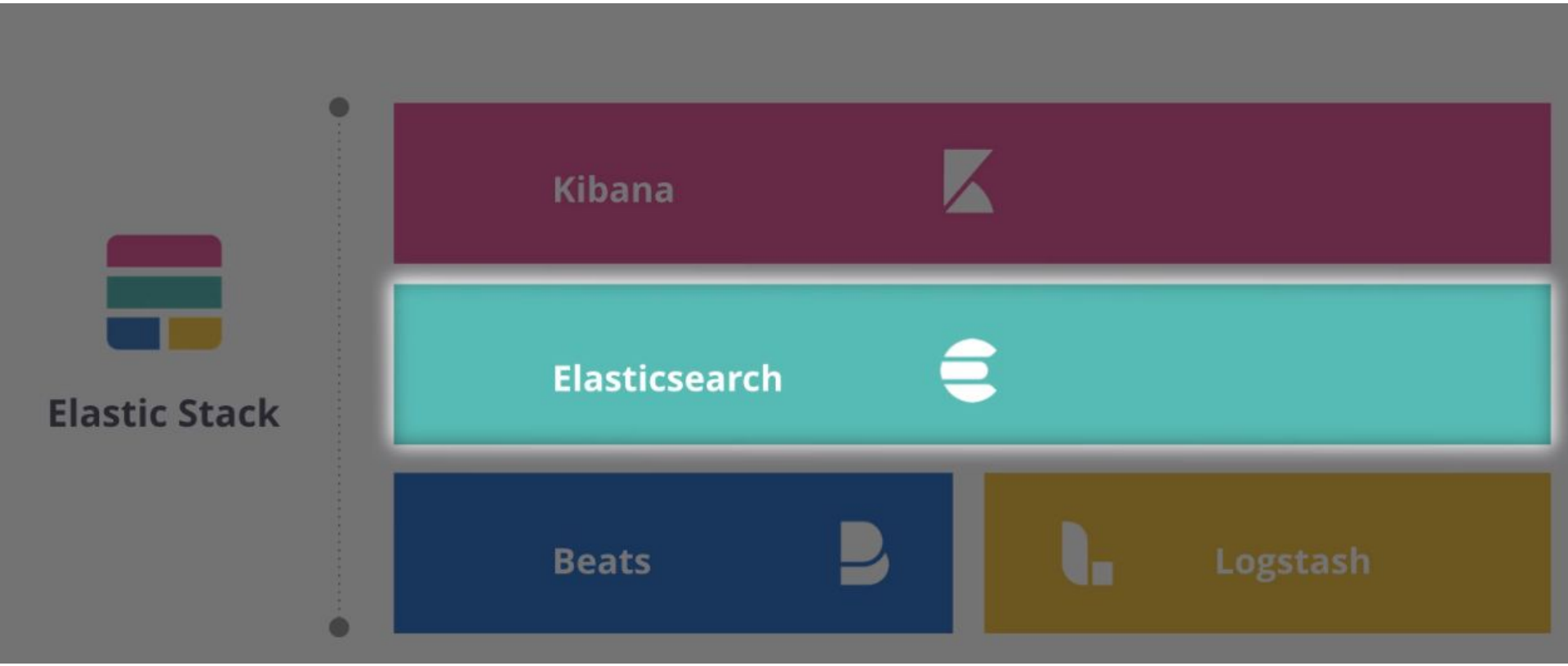
Centralização de Logs

- 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
Kibana
Visualize & Manage
Elasticsearch
Store, Search, & Analyze
Beats
Logstash
Ingest
Elastic Stack
SaaS
Elastic cloud
SELF-MANAGED
Elastic cloud Enterprise
Standalone

ELASTICSEARCH



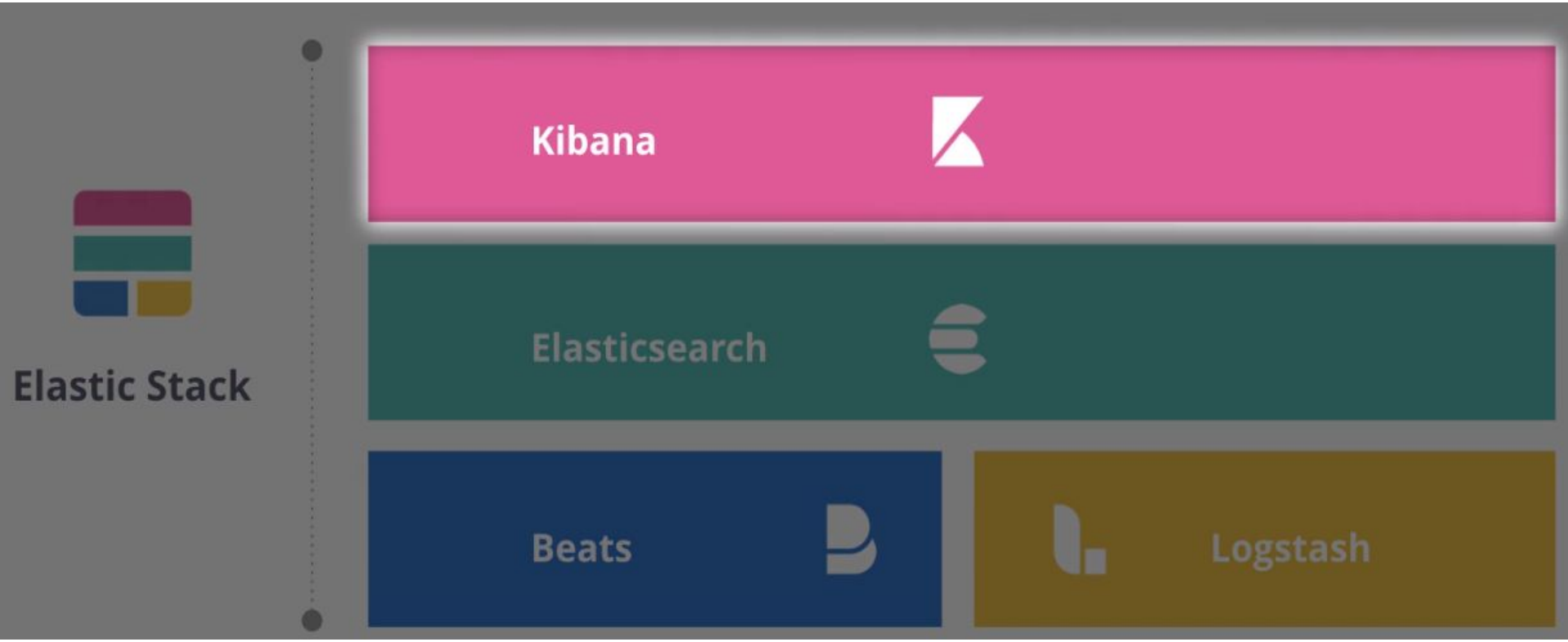
Elasticsearch

- 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

Elasticsearch

- 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)

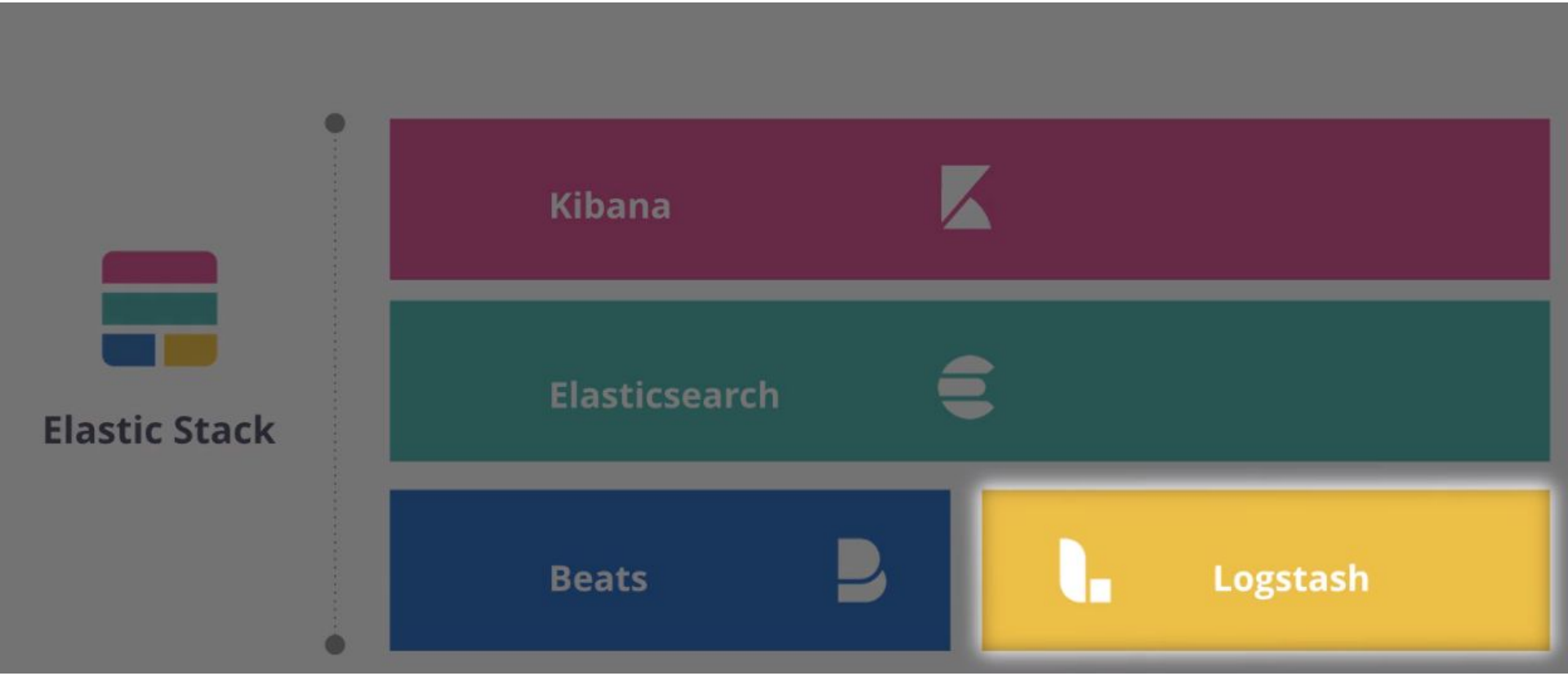
KIBANA



Kibana

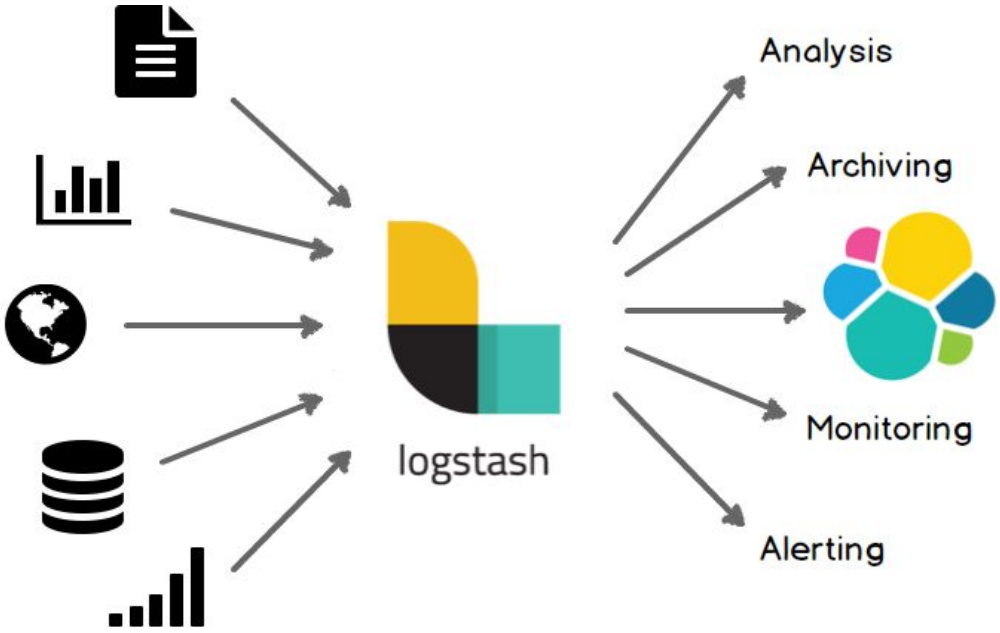
- Ferramenta analítica
- Interface Web para pesquisa e visualização (consultas e filtros)
- Agregações complexas, gráficos e tabelas
- Frequentemente utilizado para análise de LOGs (adeus grep!)
- Interação com os índices e exploração sem escrita de código
- Trabalha com dados em tempo real
- Gerência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

LOGSTASH

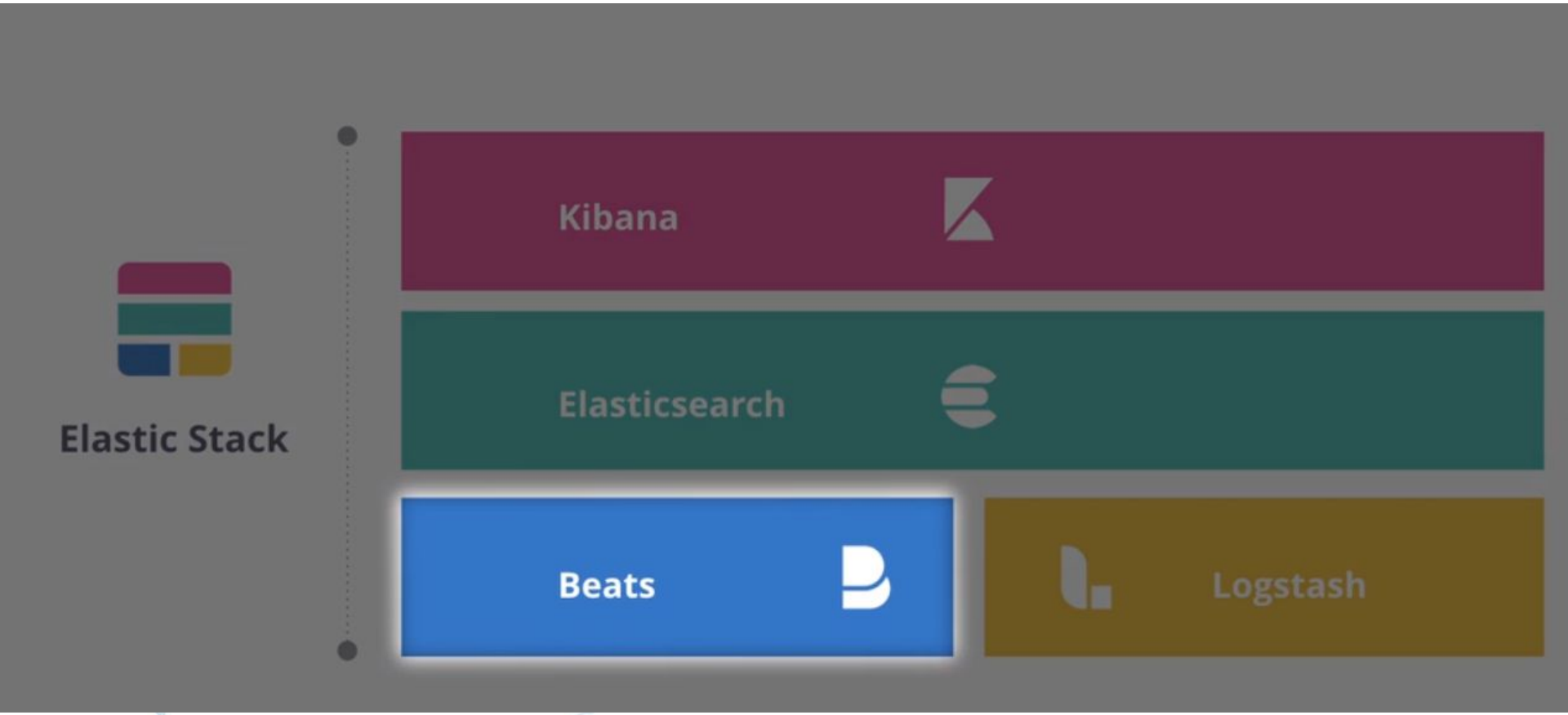


Logstash

- 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



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

elastic

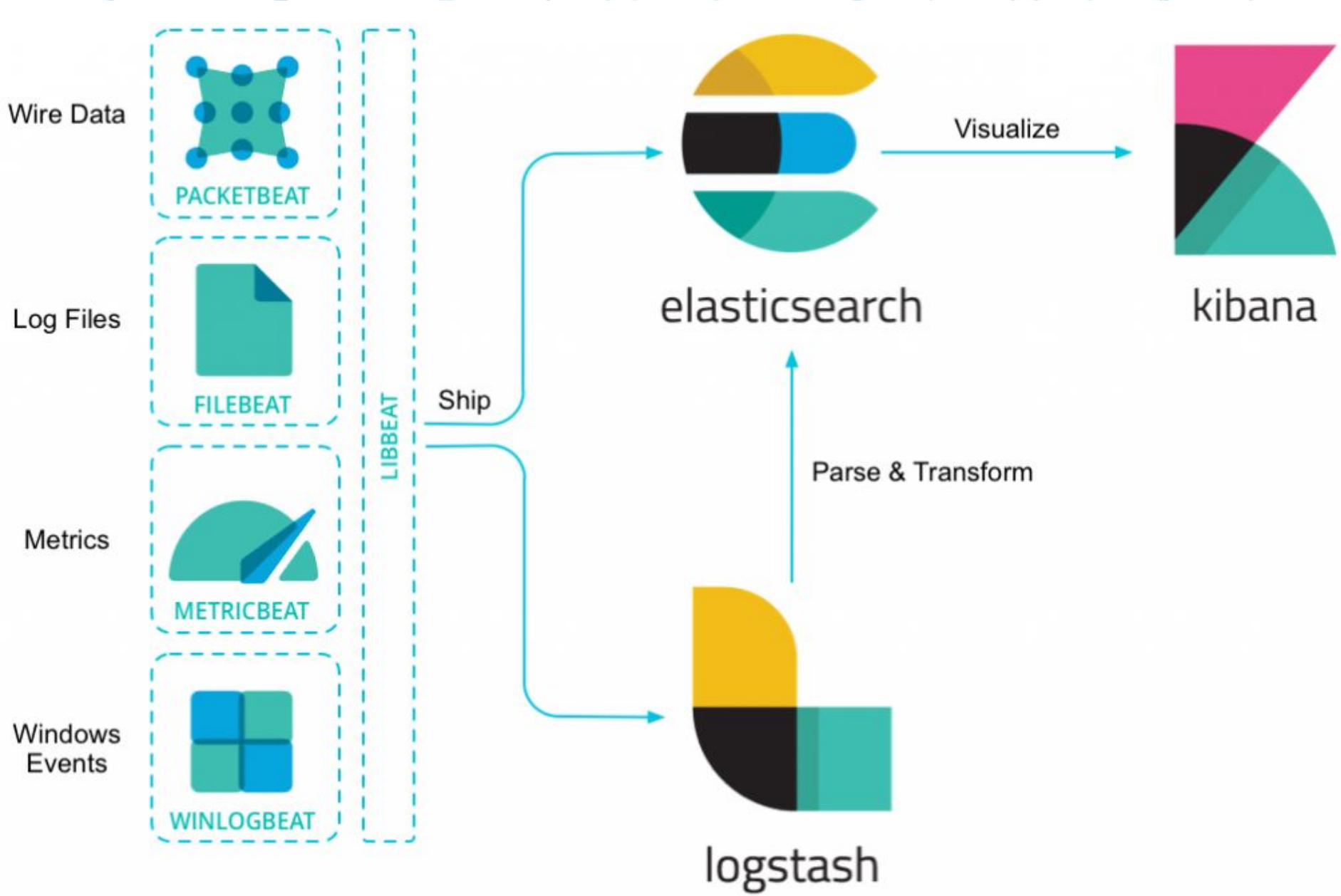
Filebeat

- 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

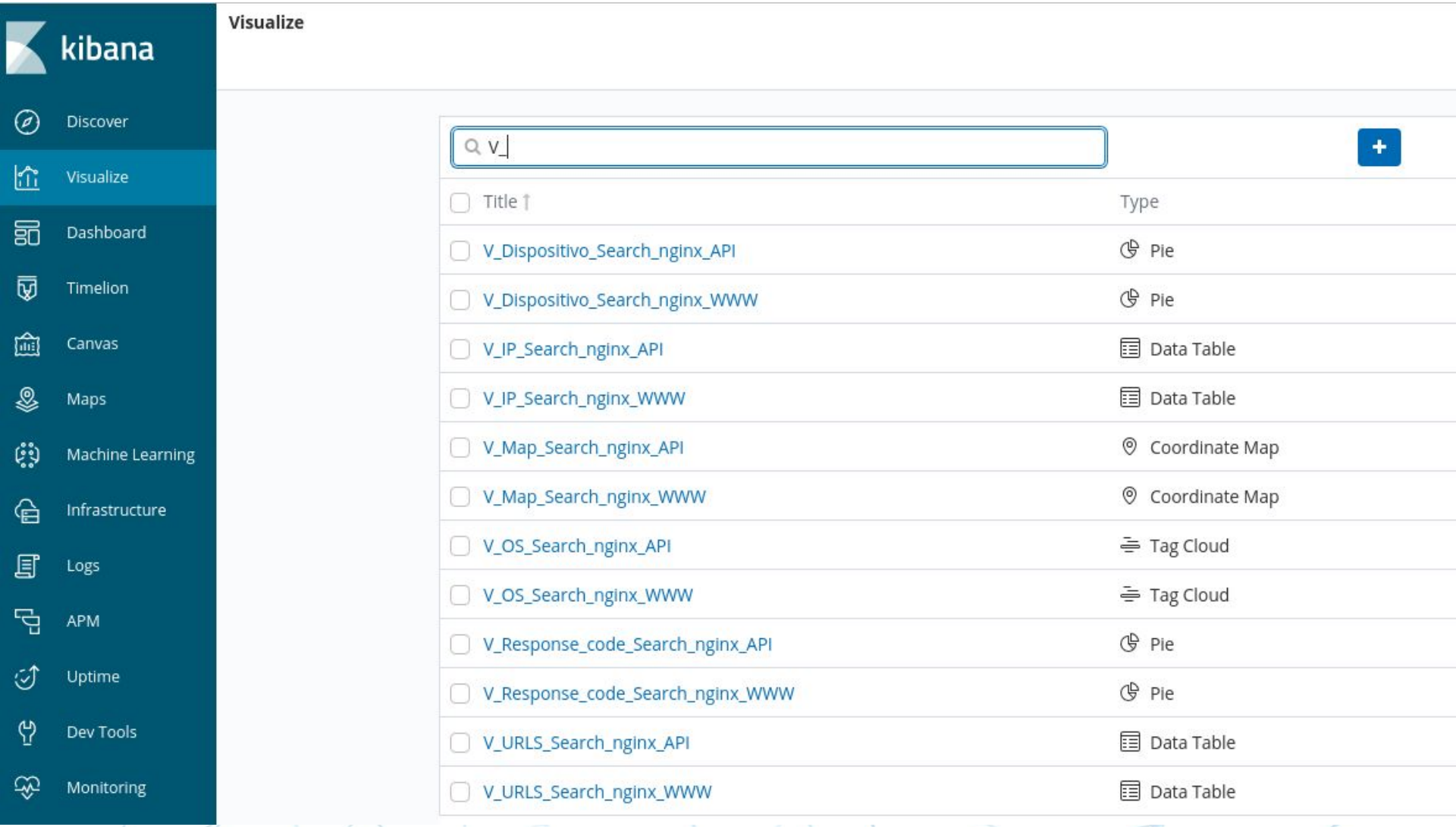
Elasticsearch - Instalação

- 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

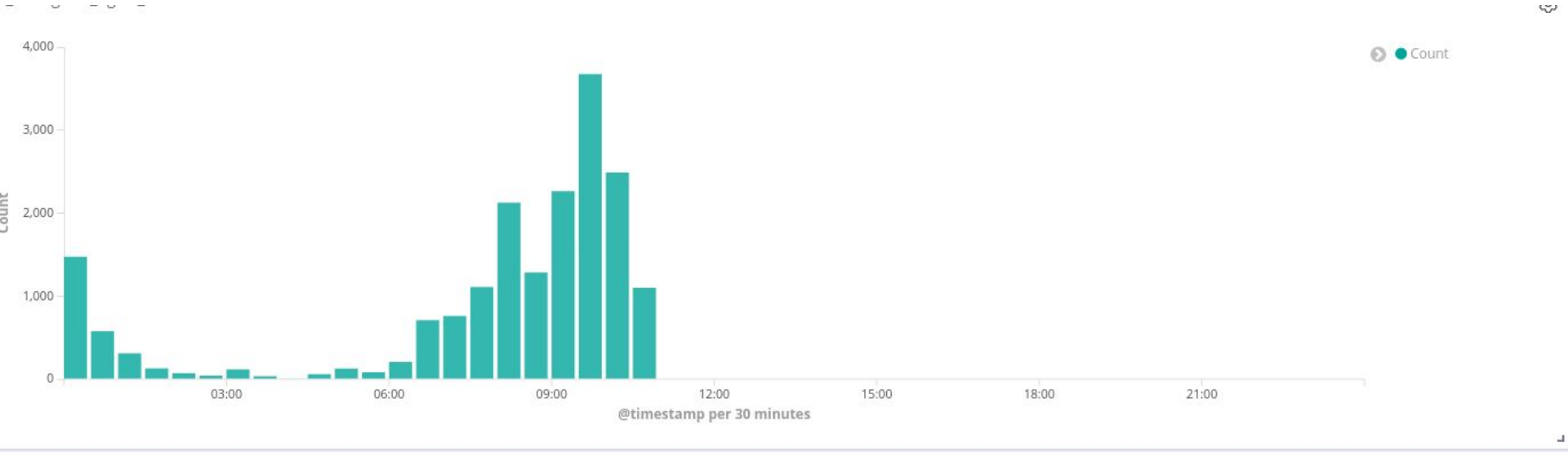
Criando Dashboards no Kibana

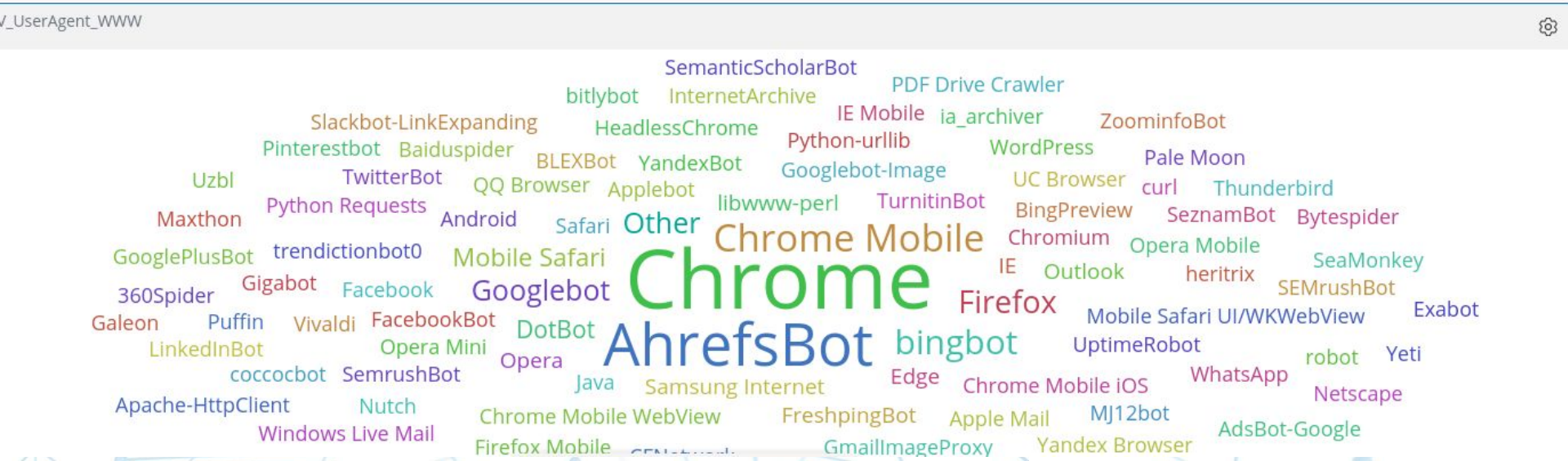
- Criar e salvar a pesquisa
- Criar os diversos gráficos de visualização vinculado à pesquisa salva
- Criar a dashboard agrupando os gráficos
- Criar novas pesquisa e copiar os gráficos associando à essa nova pesquisa através da edição de objetos no Kibana

Visualizações

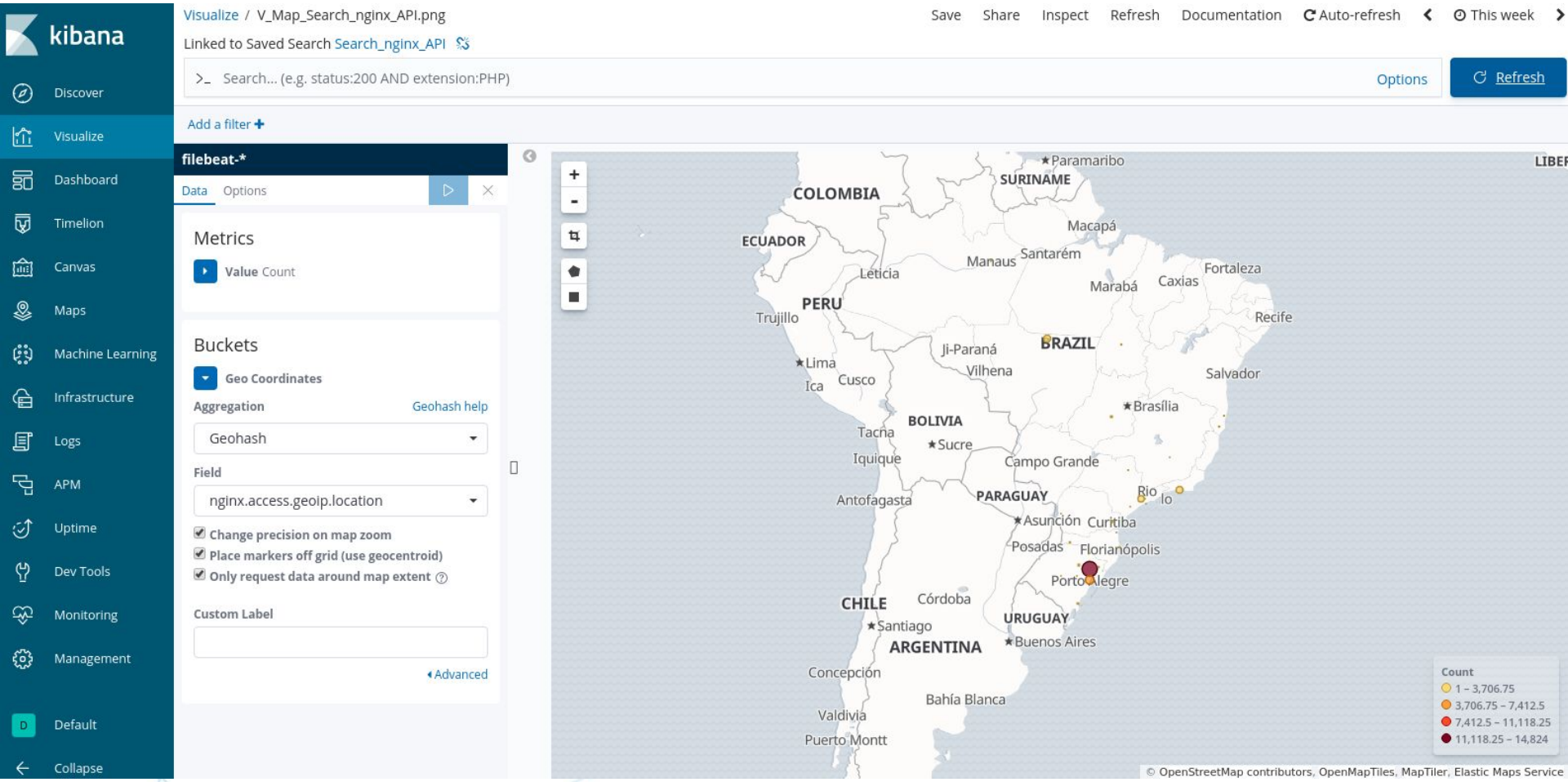


Acessos por User-agent

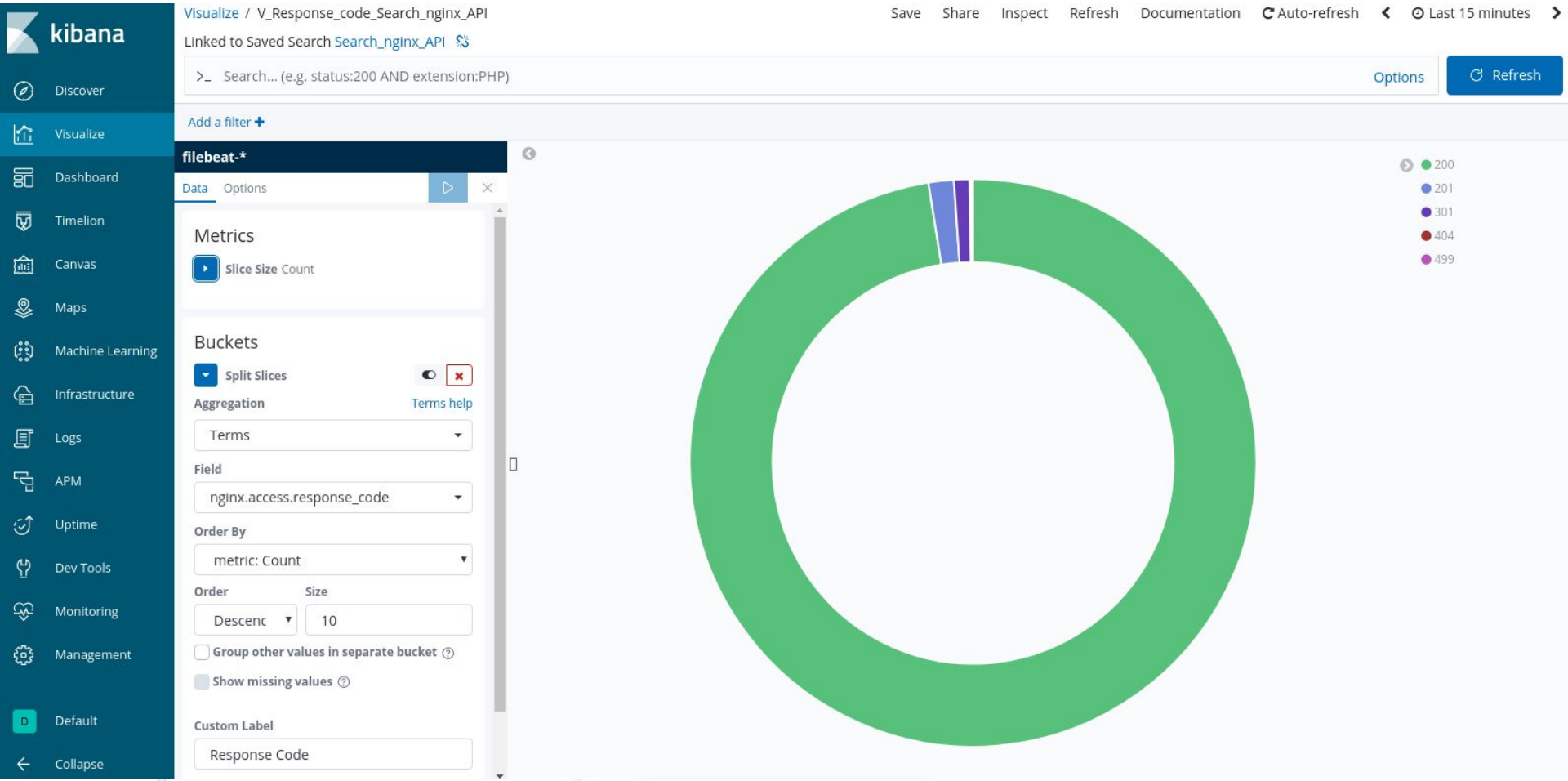




Acessos por Geolocalização



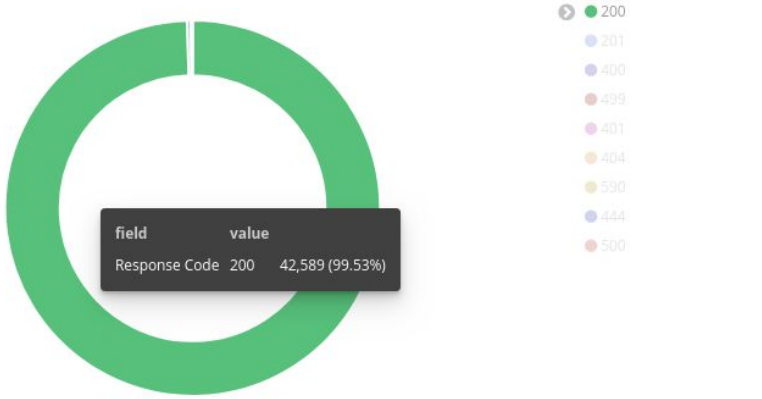
Acessos por HTTP Response



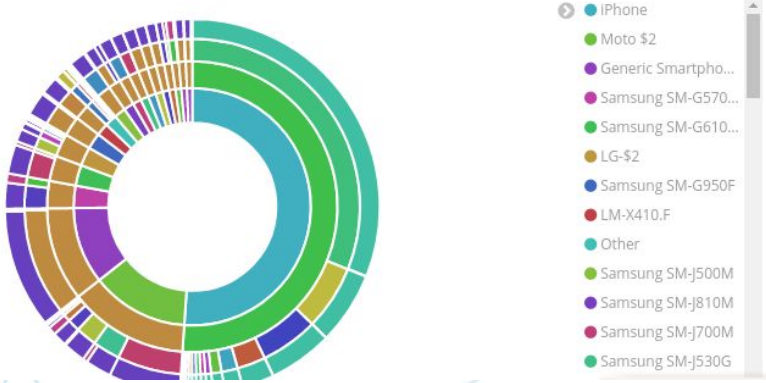
Dasboard - Acessos à API

V_Map_Search_nginx_API.png

V_Response_code_Search_nginx_API



V_Dispositivo_Search_nginx_API



V_OS_Search_nginx_API

kibana

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

Count - nginx.access.user_agent.os: Descending

V_URLS_Search_nginx_API

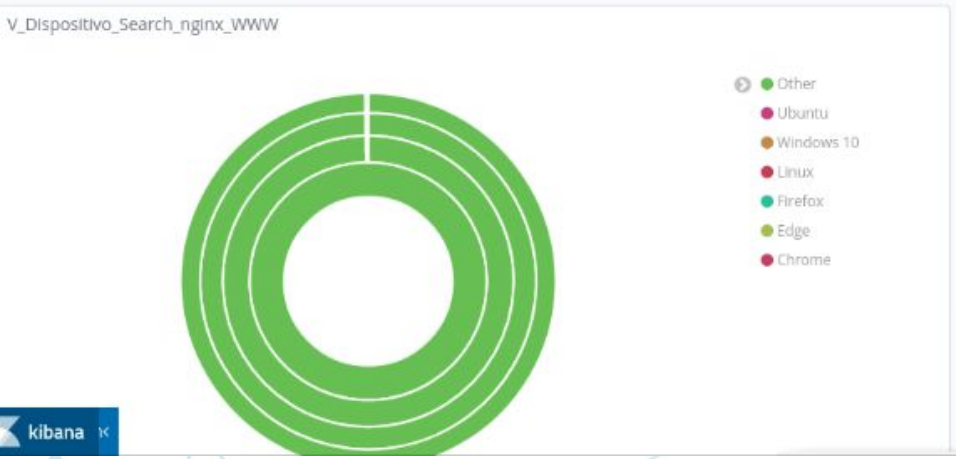
URL	Count
	2,363
	2,356
	2,318
	2,246
	2,241
	2,158
	2,155
	1,817
	310
	277

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



Identificando um Ataque

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/info.cgi	16

V_IP_Search_nginx_WWW

IP	Count
174.128.225.10	6,045

Filter for value

kibana

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']
        ))
```

UCS
UNIVERSIDADE
DE CAXIAS DO SUL

Configurando o Frontend Nginx

FUNDAÇÃO UNIVERSIDADE
DE CAXIAS DO SUL

badbots.conf

```
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;
 }
```

Interceptação de Erros / Limite de Req.

```
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;
    }
}
```

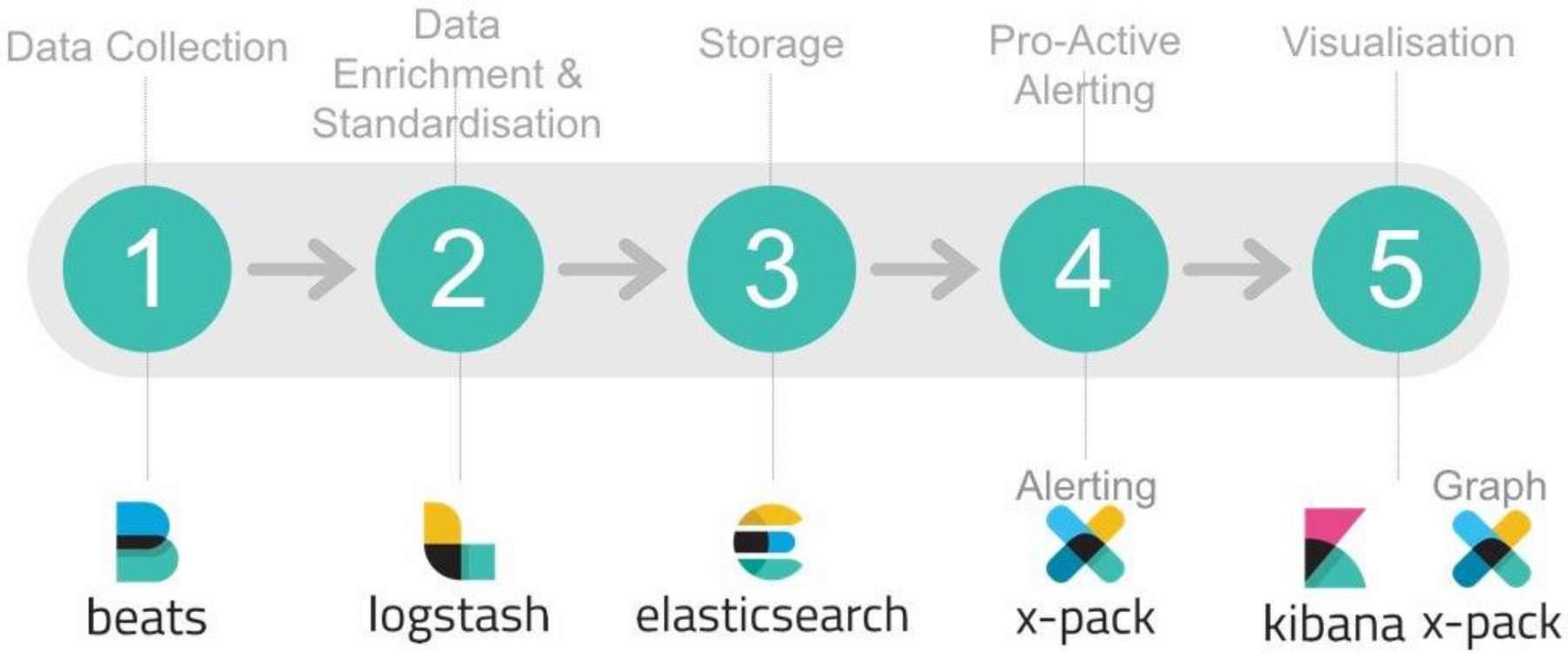
Elastic Stack

Opções de Subscrição

	GRATUÍTO		SUBSCRIÇÃO		
	OPEN SOURCE	BASIC	GOLD	PLATINUM	ENTERPRISE
SELF-MANAGED	Open Source Features	Free Proprietary Features	Paid Proprietary Features Elastic Support		Elastic Cloud Enterprise Elastic Support

	SUBSCRIÇÃO		
	ELASTIC CLOUD		
SaaS	Elasticsearch Service	Elastic App Search Service	Elastic Site Search Service

Security and Threat Detection with the Elastic Stack



X-Pack

- 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)

X-Pack Features

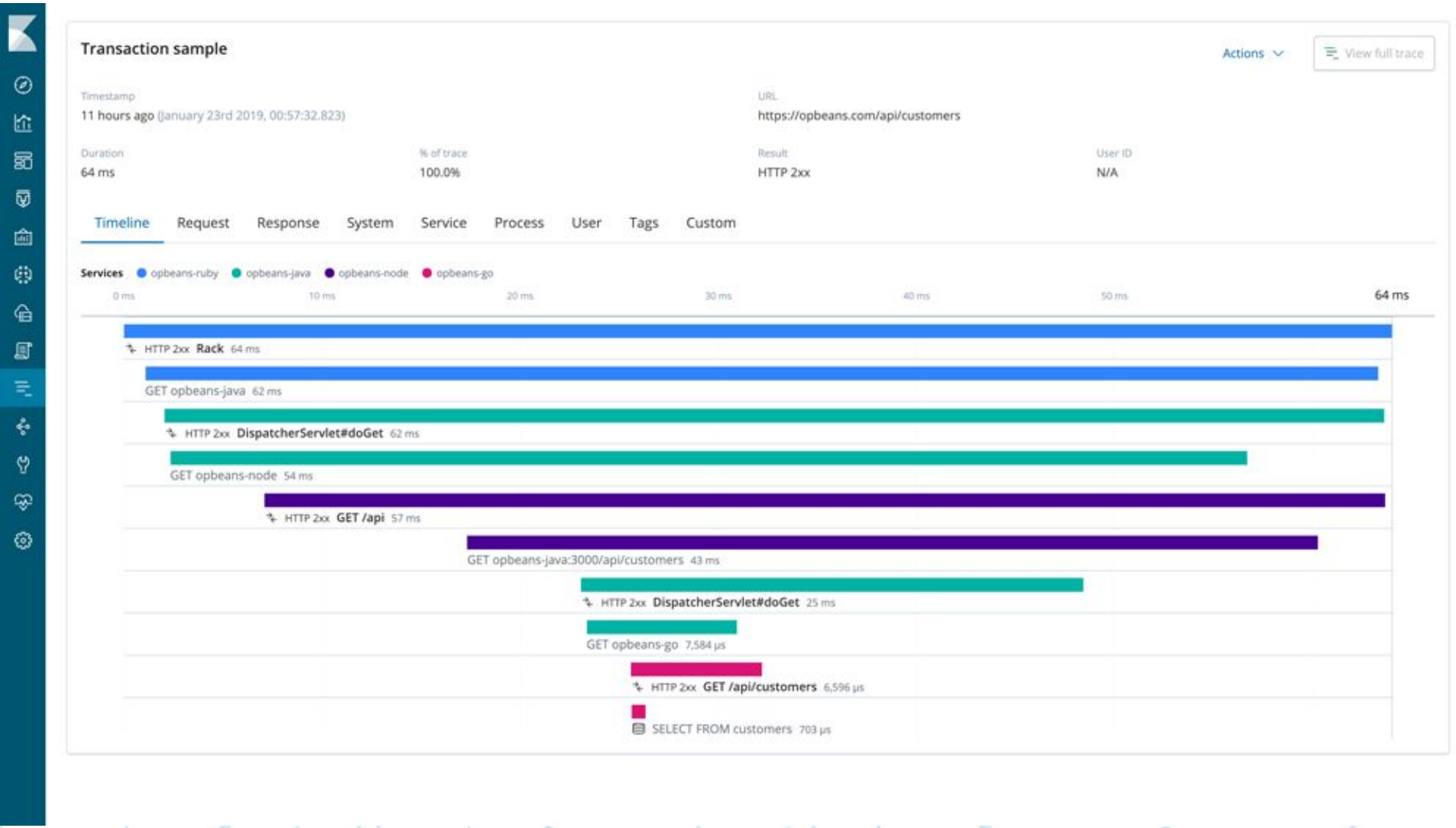
Subscriptions

Free X-Pack features included in Basic

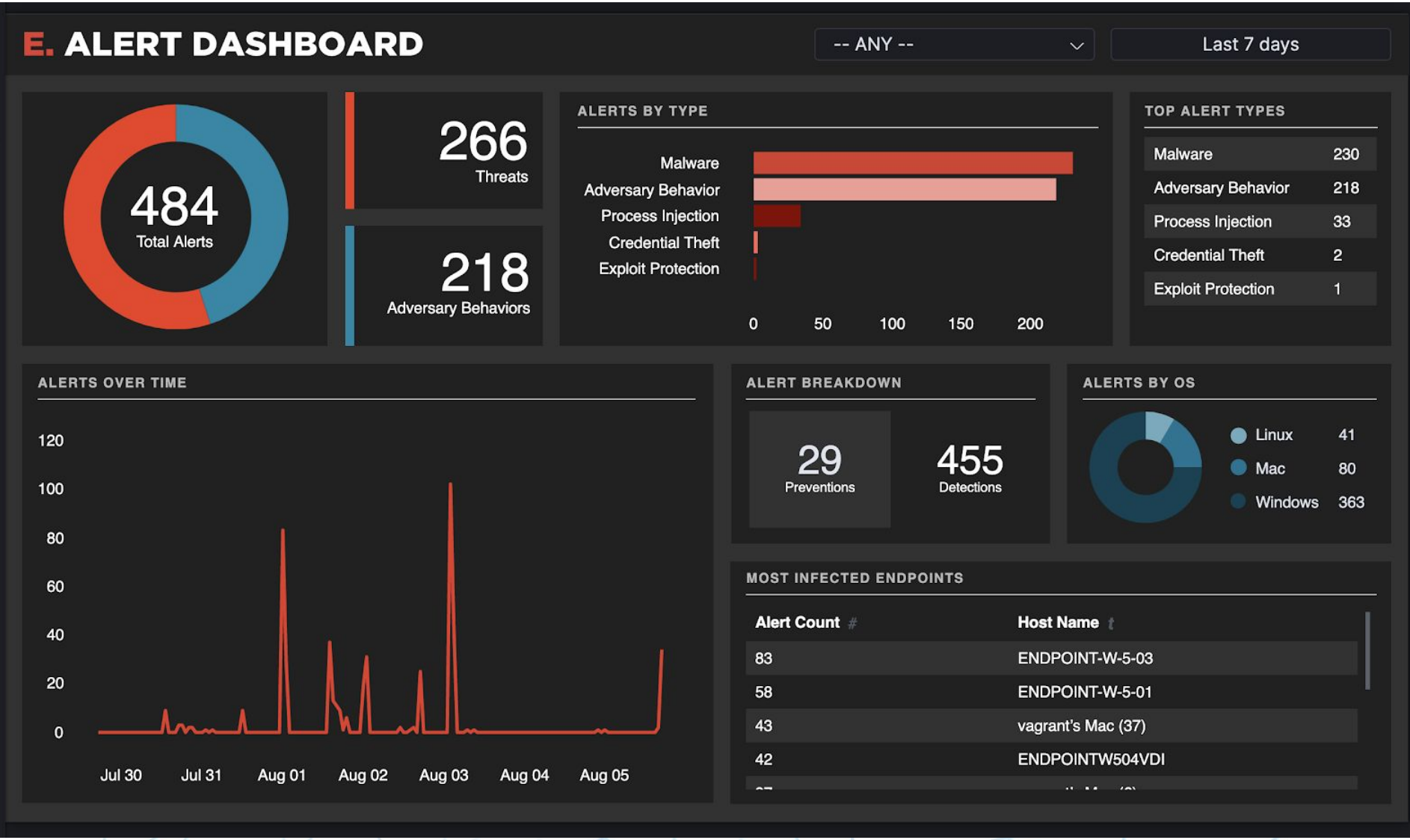
Elastic Support included in Gold, Platinum, and Enterprise Subscriptions

	OPEN SOURCE Free Download	BASIC Free License	GOLD Request Info	PLATINUM Request Info	ENTERPRISE 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		✓	✓	✓	✓

Elastic APM - Application Performance Monitoring



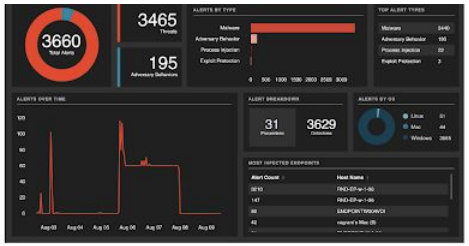
Canvas Dashboards



UCS
UNIVERSIDADE
DE CAXIAS DO SUL

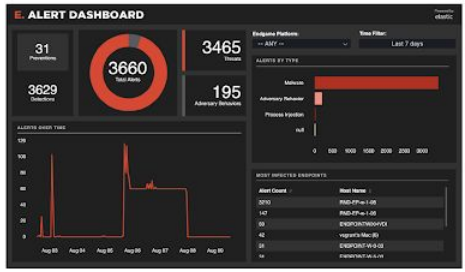
Canvas - Endgame









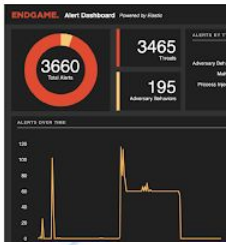




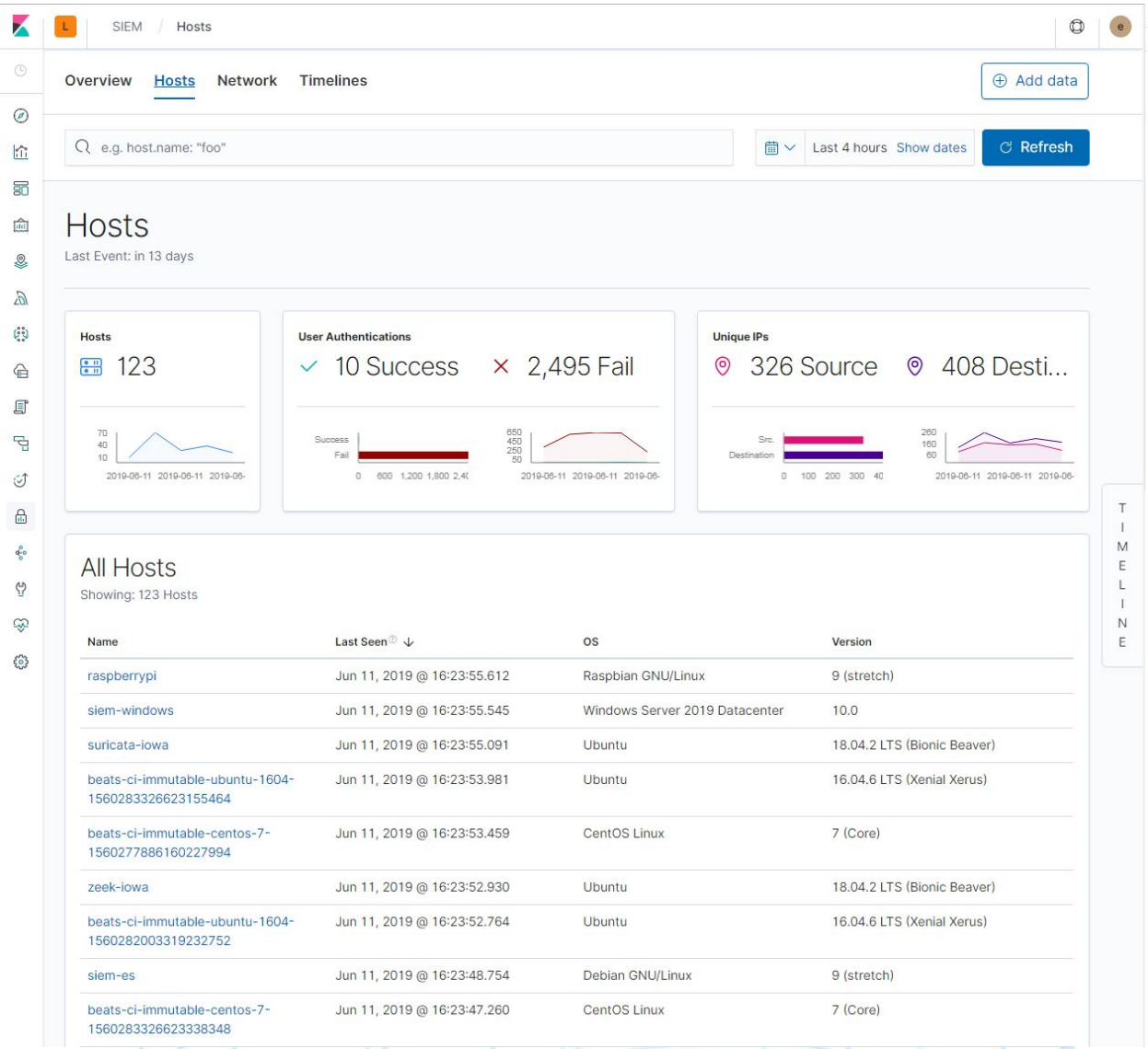


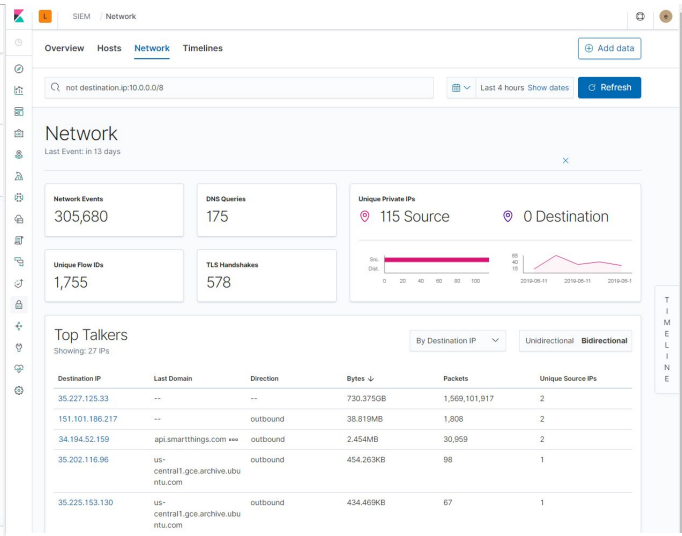






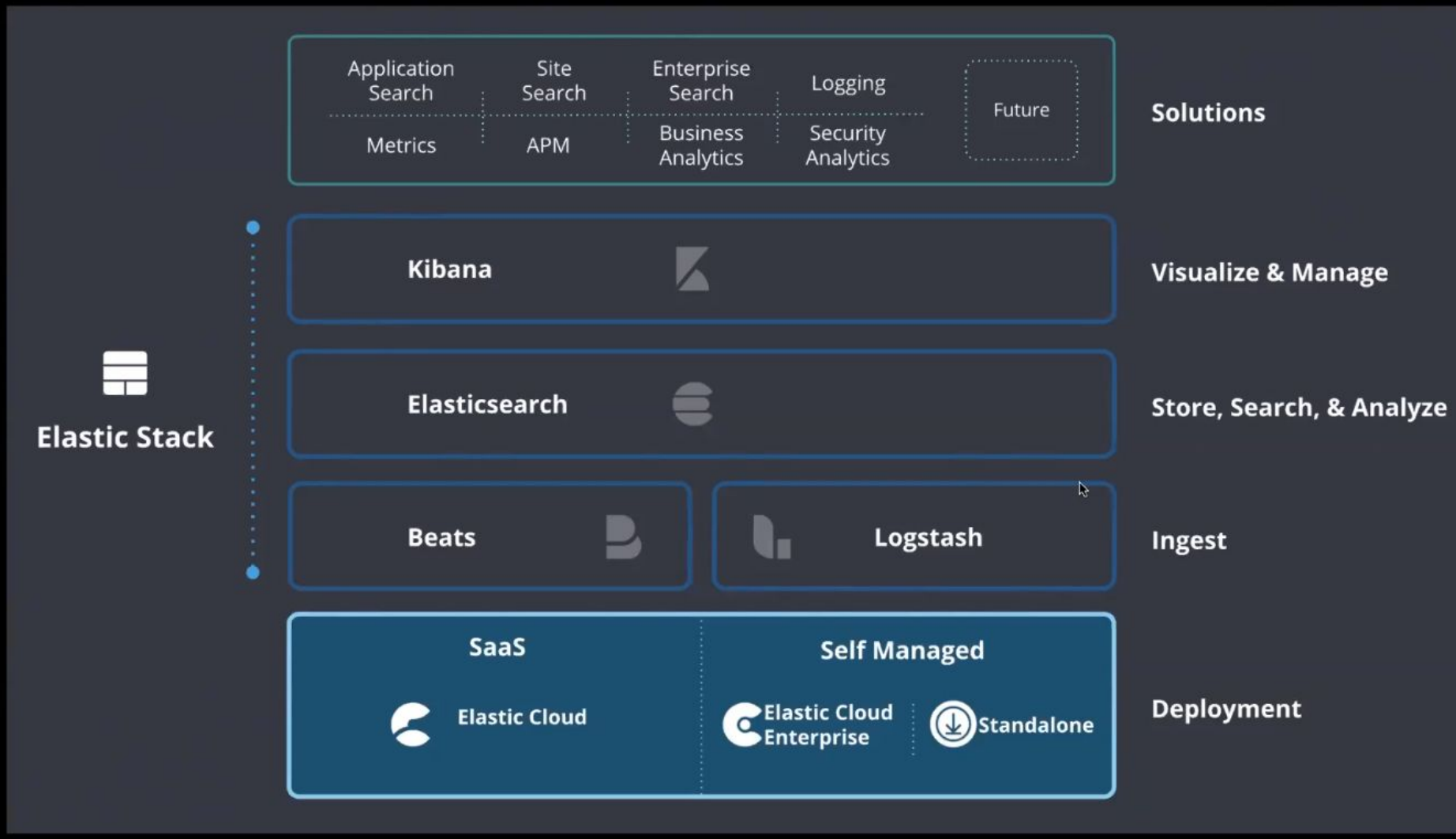
Elastic SIEM





FUNDAÇÃO UNIVERSIDADE DE CAXIAS DO SUL

Elastic Stack - Deploy



UCS UNIVERSIDADE DE CAXIAS DO SUL

Elastic Stack - Subscrptions

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

Vazamentos de Bases Elasticsearch

- Novembro/2018 - 57 milhões de cidadãos americanos expostos encontrados por um scan via Shodan
- Maio/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

Referências

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

Agradecimentos

- 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