OSSE{LK}C

Rodrigo Montoro
Pesquisador / Security Operations Center (SOC)
rodrigo@clavis.com.br

Motivação

- Compliance
- Cansado de "grepear"
- Flexibilidade
- Pesquisas retroativas
- Correlação com outras fontes de dados
- Diminuir a janela de exposição

$ whoami

- Pesquisador / SOC Clavis Security
- Autor de 2 pesquisas com patenteadas
- Palestrante diversos eventos Brasil, EUA e Canadá
- Evangelista Opensource
- Usuário linux desde 1996
- Pai
- Triatleta / Corredor trilhas

OCTOPUS

SECURITY INFORMATION AND EVENT MANAGEMENT

Agenda

- OSSEC
- Elastic Stack
- Integrando OSSEC + ELK
- Demonstração
- Conclusões / Dicas

CLAVIS
segurança da informação

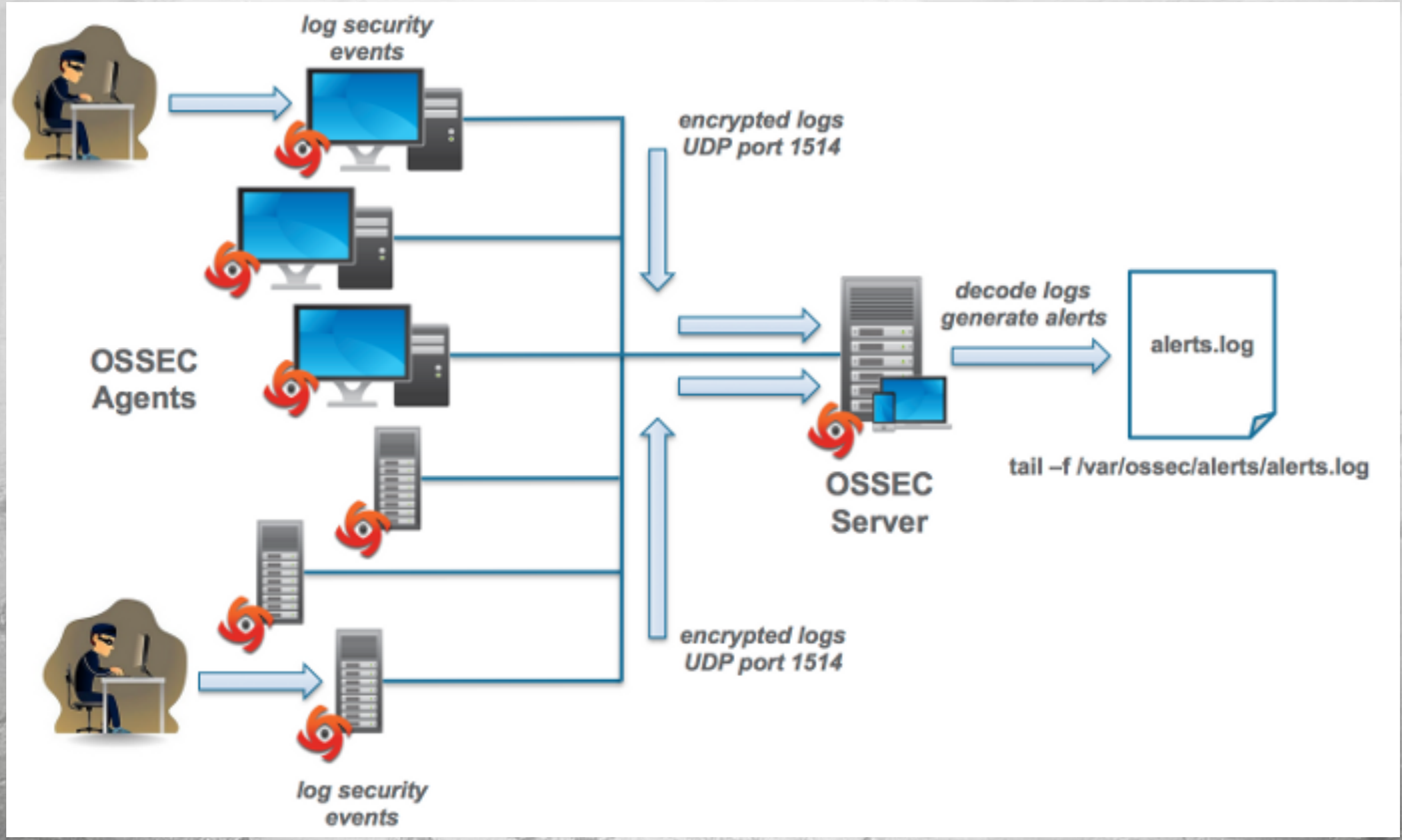
Funcionalidades

- Análise de logs
- Integridade de arquivos (FIM)
- Monitoramento registros (Windows)
- Detecção malwares / rootkits
- Checagem baselines / hardening (CIS)
- Multiplataforma
- Reposta ativa

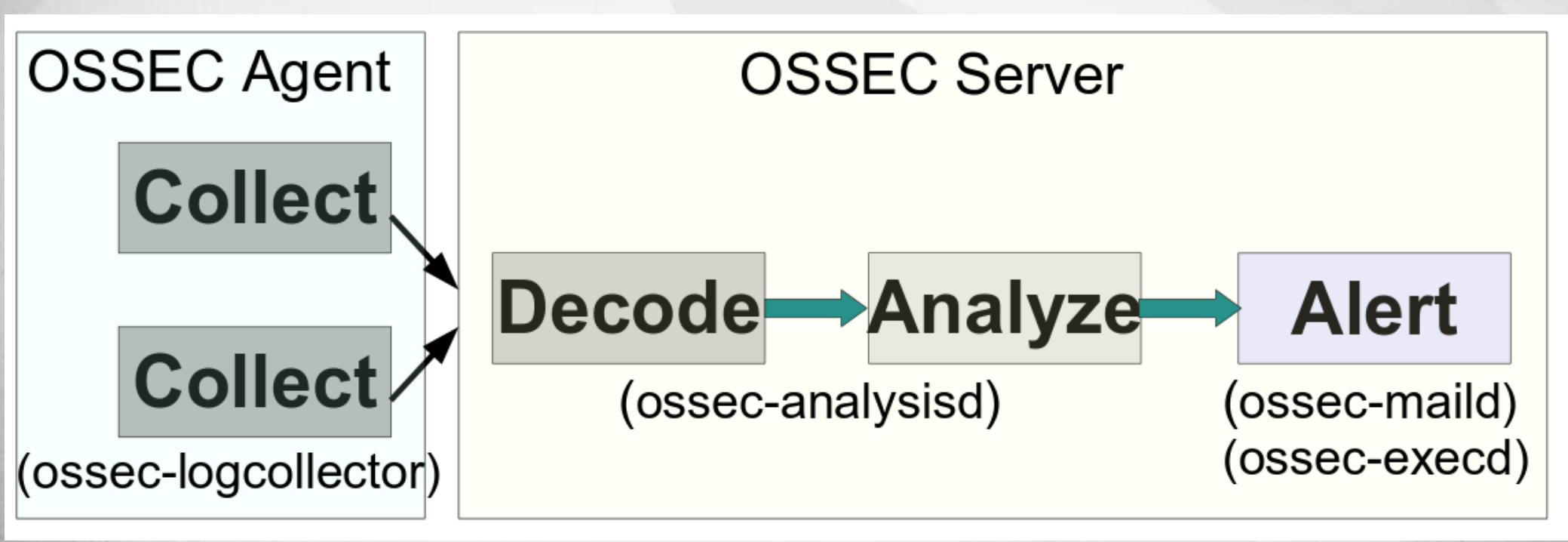
Modos funcionamento

- Local
- Agente
- Servidor

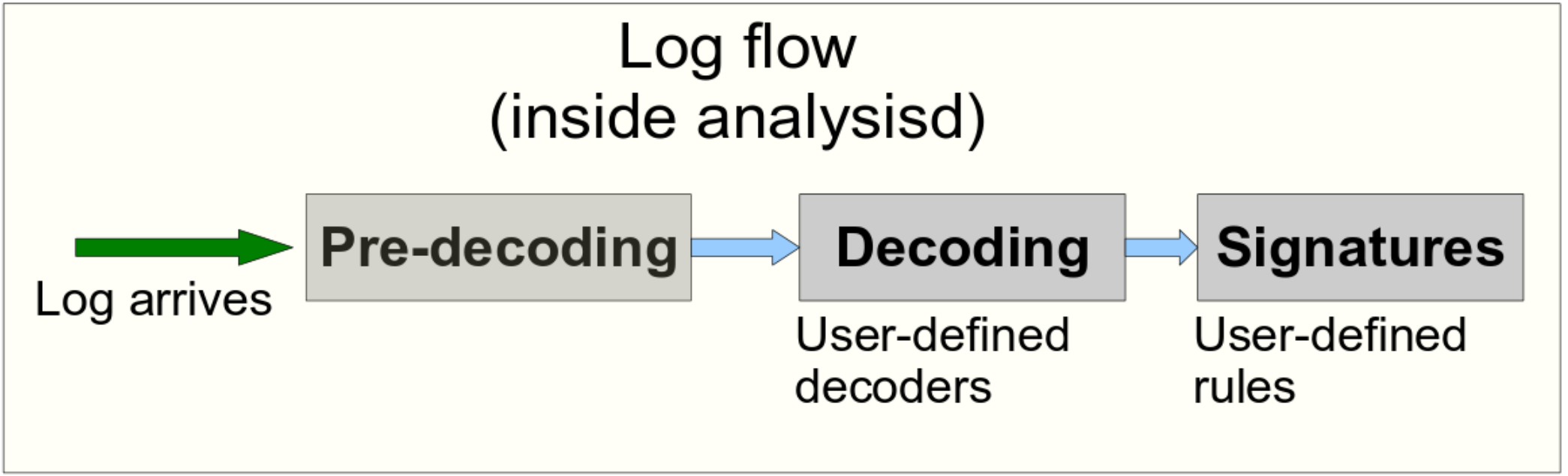
Visão Geral



Fluxo OSSEC



analysisd internals



ossec-logtest

```
[root@OctopusLiveDemo ~]# /var/ossec/bin/ossec-logtest
2016/05/13 01:39:02 ossec-testrule: INFO: Reading local decoder file.
2016/05/13 01:39:02 ossec-testrule: INFO: Started (pid: 13694).
ossec-testrule: Type one log per line.

May 13 01:24:39 eventidlabs sshd[26834]: Failed password for root from 183.3.202.113 port 26063 ssh2


**Phase 1: Completed pre-decoding.
       full event: 'May 13 01:24:39 eventidlabs sshd[26834]: Failed password for root from 183.3.202
.113 port 26063 ssh2'
       hostname: 'eventidlabs'
       program_name: 'sshd'
       log: 'Failed password for root from 183.3.202.113 port 26063 ssh2'

**Phase 2: Completed decoding.
       decoder: 'sshd'
       dstuser: 'root'
       srcip: '183.3.202.113'

**Phase 3: Completed filtering (rules).
       Rule id: '5716'
       Level: '5'
       Description: 'SSHD authentication failed.'
**Alert to be generated.
```

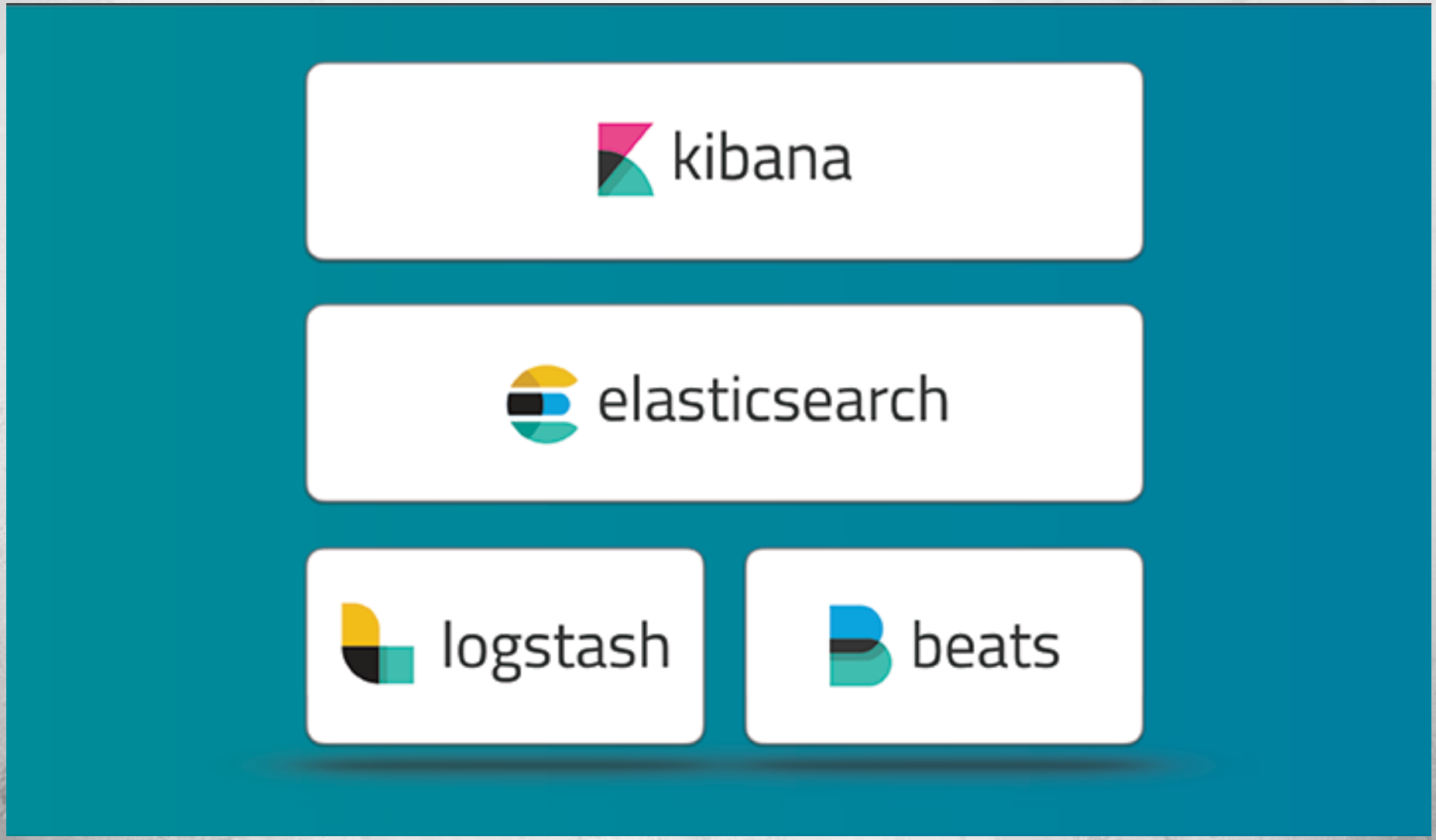
Reposta ativa (Padrão)

```
[root@OctopusLiveDemo bin]# pwd
/var/ossec/active-response/bin
[root@OctopusLiveDemo bin]# ls -1
disable-account.sh
firewall-drop.sh
firewalld-drop.sh
host-deny.sh
ip-customblock.sh
ipfw.sh
ipfw_mac.sh
npf.sh
ossec-slack.sh
ossec-tweeter.sh
pf.sh
restart-ossec.sh
route-null.sh
[root@OctopusLiveDemo bin]#
```

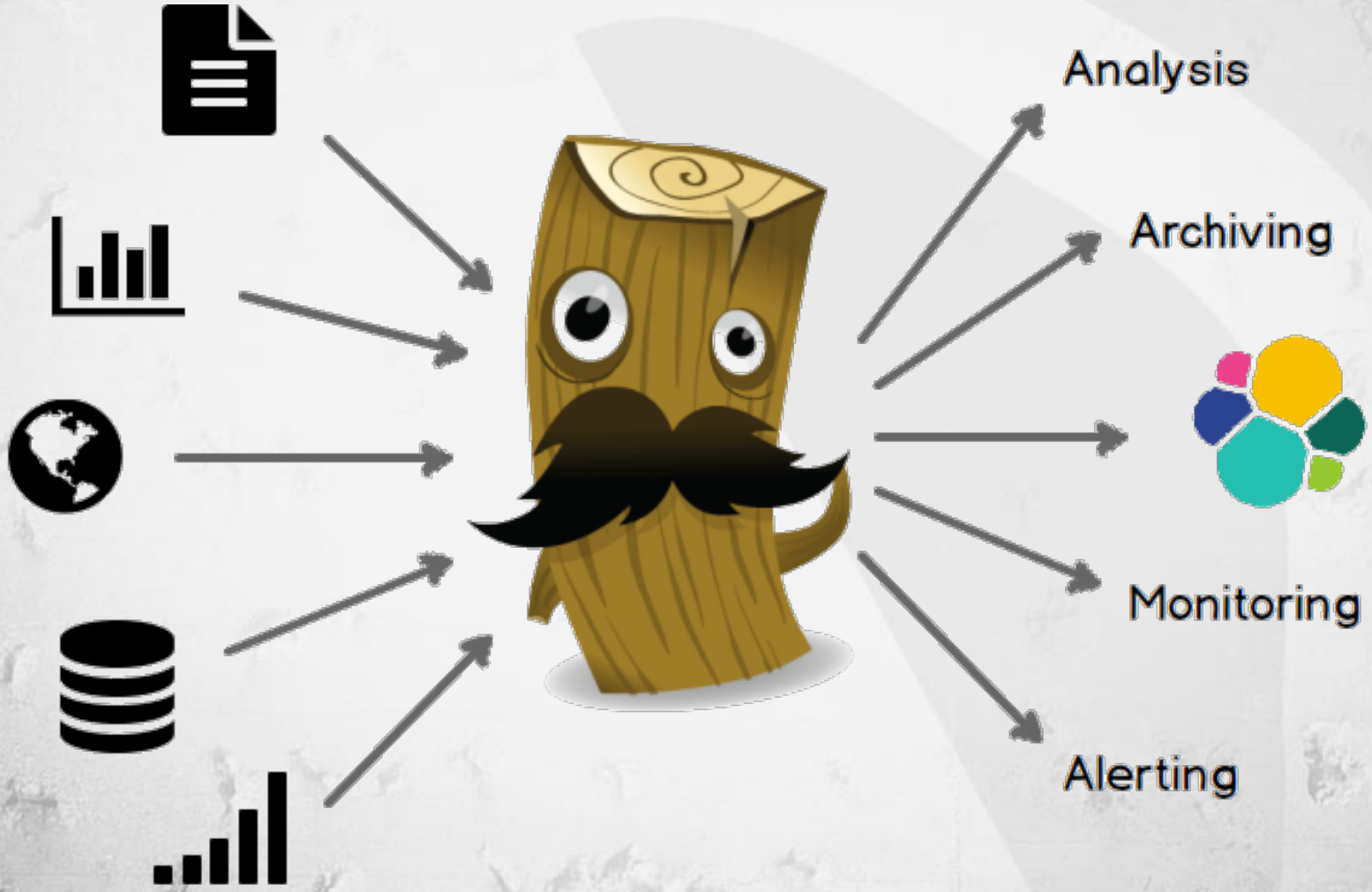
Exemplo de Resposta Ativa

- active-response/virustotal_lookup.sh/virus_total.py - Look up hash from syscheck alerts in VT database
- active-response/cymru_lookup.sh - Look up hash from sysheck alerts in Team Cymru Malware Hash Registery
- active-response/puppetdb_lookup.sh - Look up managed files in PuppetDB
- active-response/rpm_lookup.sh - Look up files that changed from RPM install (must be present on agents)
- active-response/deb_lookup.sh - Lookup file that changes from DEB install (must be present on agents)
- active-response/time_lookup.sh - Check if system clock is off or time zone differs for analyzed logs
- active-response/ldap_lookup.sh - Lookup employee usernames in LDAP database
- active-response/command_search.sh - Search for malicious commands across logs
- active-response/cif.sh - Create intelligence feed from alerts
- active-response/bhr.sh - Block hosts at perimeter using Black Hole Router by Justin Azoff
- active-response/add_to_cdb.sh - Add entries from alerts to CDB database (only collect system users at this time)
- active-response/rule-all.sh - Run many of the above scripts
- active-response/syscheck-all.sh - Run many of the syscheck scripts

Elastic Stack



Logstash



Elasticsearch (1/2)

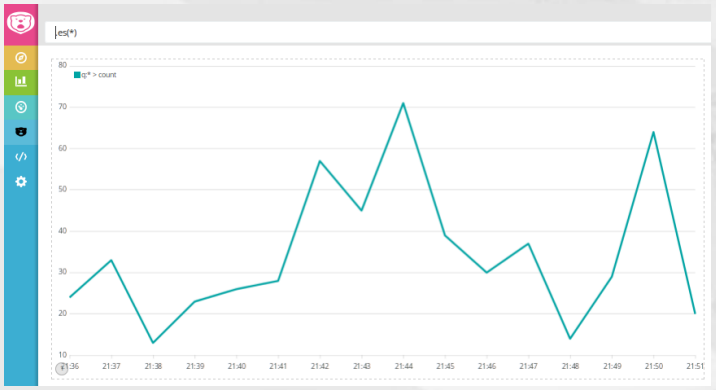
- Open source
- Distribuido
- Full text search engine
- Baseado no Apache Lucene
- Rápido acesso a informação
- Dados salvos no formato JSON

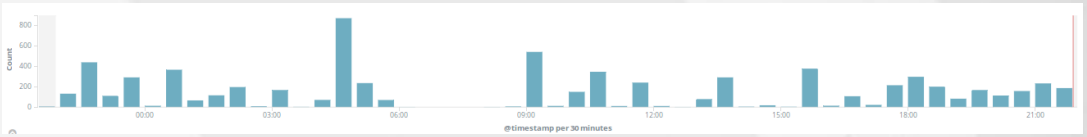
Elasticsearch (2/2)

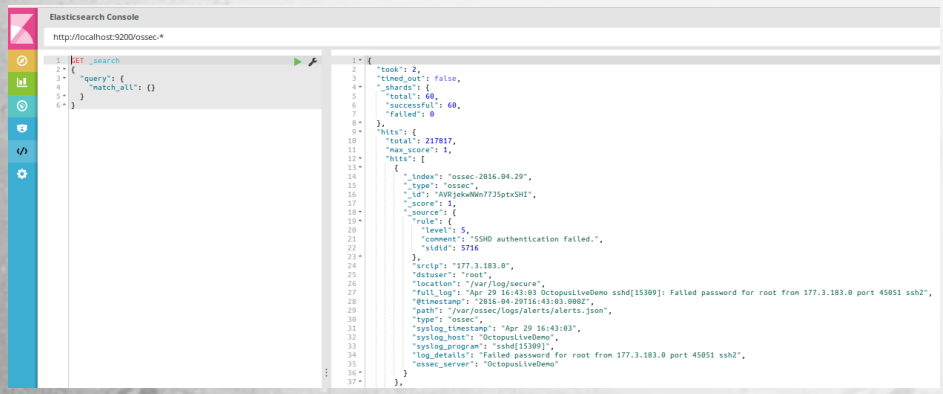
- Suporta sistemas único ou múltiplos nodes
- Fácil de configurar e escalável
- Possui uma RESTful API
- Fácil criação snapshots / backups
- Instalação disponível em diversos formatos

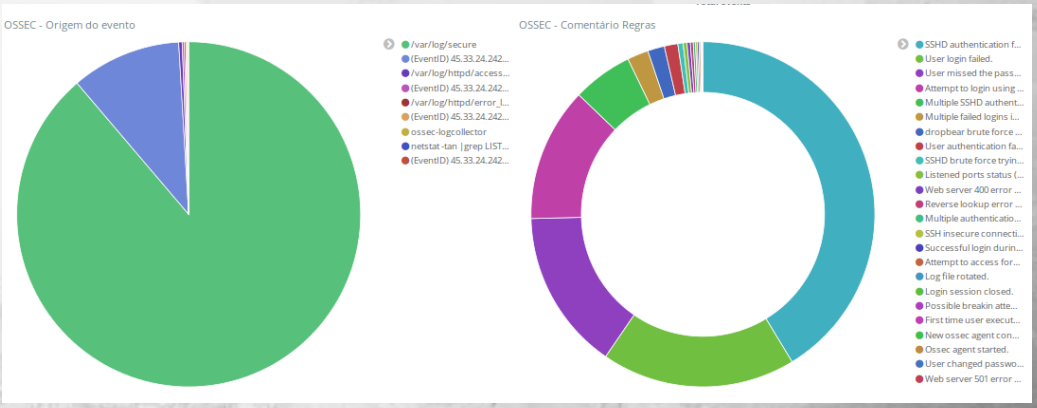
Kibana

- Explore
- Visualize
- Descubra





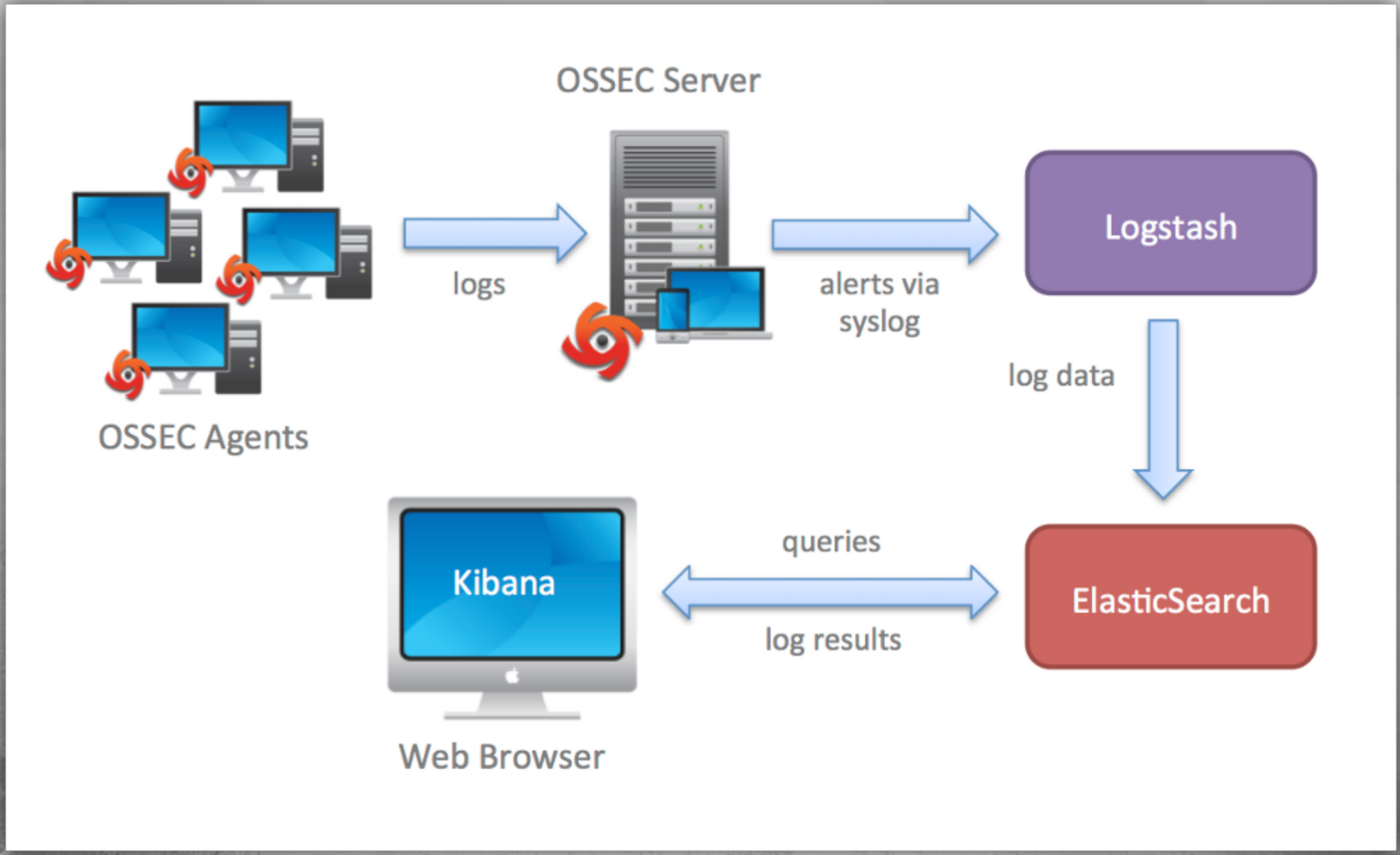




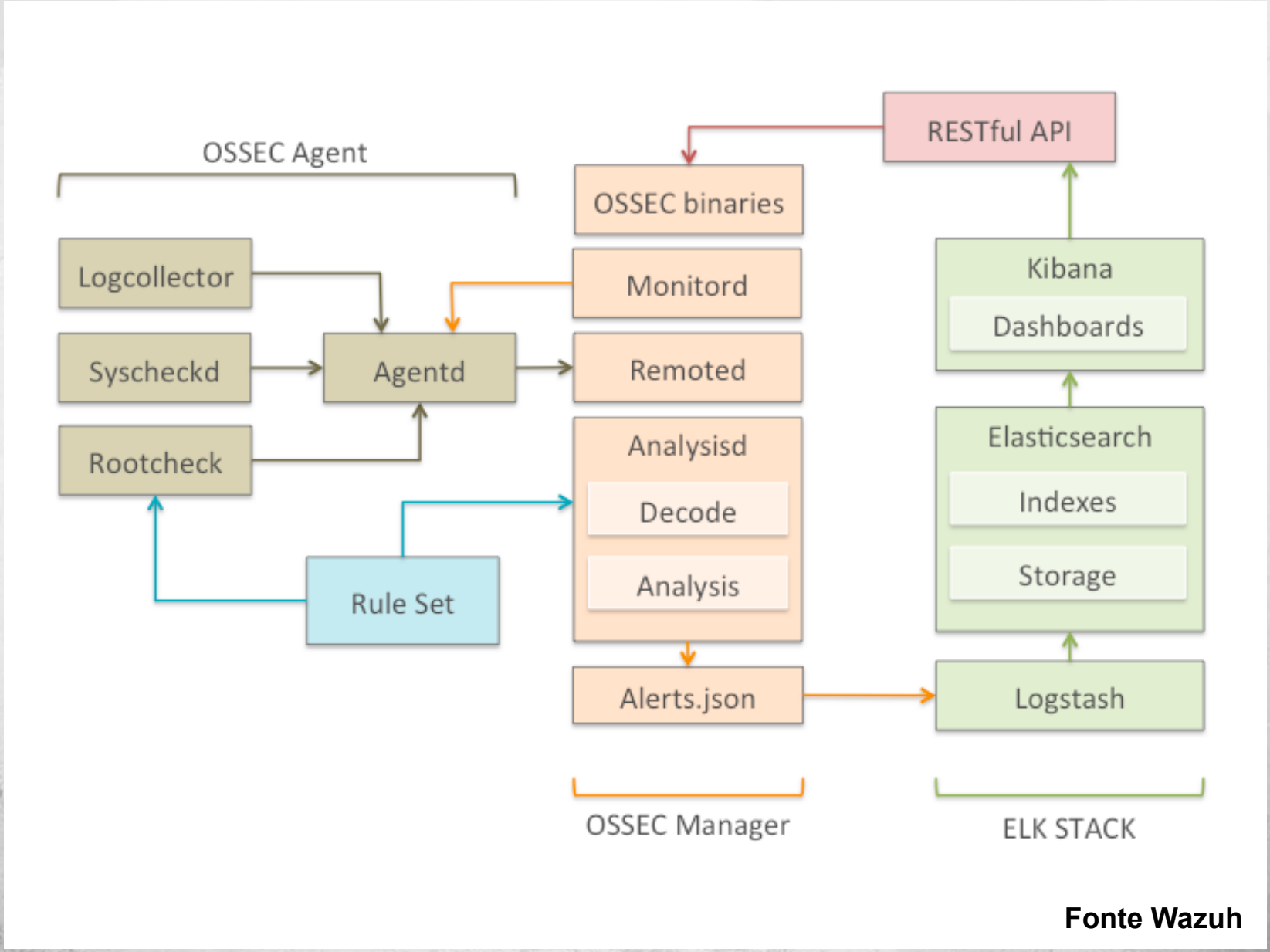
OSSEC + ELK

$$\bar{x} = \frac{\sum_{i=1}^{N} x_i}{N}$$

Fluxo integração



Integração Internals



Fonte Wazuh

Demostração Kibana

Exemplo alerta (1/3)

Table JSON

Link to /ossec-2016.05.13/ossec/AVSnmyxAiL5o0e6UWqtU

@timestamp	May 12th 2016, 21:54:04.473
t _id	AVSnmyxAiL5o0e6UWqtU
t _index	ossec-2016.05.13
# _score	-
t _type	ossec
t full_log	ossec: output: 'netstat -tan |grep LISTEN |egrep -v '(127.0.0.1| \\1)' | sort': tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:65000 0.0.0.0:* LISTEN tcp6 0 0 :::1510 :::* LISTEN tcp6 0 0 :::22 :::* LISTEN tcp6 0 0 :::65000 :::* LISTEN
t location	(EventID) 45.33.24.242->netstat -tan |grep LISTEN |egrep -v '(127.0.0.1| \\1)' | sort
t ossec_server	OctopusLiveDemo
t path	/var/ossec/logs/alerts/alerts.json
t rule.comment	Listened ports status (netstat) changed (new port opened or closed).
# rule.level	7
# rule.sidid	533
t type	ossec

Facilitando a análise ...

```
[root@eventidlabs ~]# ausearch -k backdoor_success -i
----
type=PROCTITLE msg=audit(05/13/16 00:40:14.269:923635) : proctitle=nc -l 65000
type=SYSCALL msg=audit(05/13/16 00:40:14.269:923635) : arch=x86_64 syscall=listen
success=yes exit=0 a0=0x3 a1=0xa a2=0x80 a3=0x7ffeab269ef0 items=0 ppid=26396 pid=
26426 auid=elkuser uid=elkuser gid=elkuser euid=elkuser suid=elkuser fsuid=elkuser
 egid=elkuser sgid=elkuser fsgid=elkuser tty=pts0 ses=3756 comm=nc exe=/usr/bin/nc
at key=backdoor_success
----
```

```
[root@eventidlabs ~]# auditctl -l
-a always,exit -F arch=b64 -S listen -F key=backdoor_success
-a always,exit -F arch=b64 -S bind -F success=0 -F key=backdoor_attempt
```

Exemplo alerta (2/3)

Table JSON

Link to /ossec-2016.05.13/ossec/AVSntze8iL5o0e6UWrDg

@timestamp	May 12th 2016, 22:24:40.000
t _id	AVSntze8iL5o0e6UWrDg
t _index	ossec-2016.05.13
# _score	-
t _type	ossec
t full_log	May 13 01:24:40 eventidlabs yum[26813]: Installed: perl-Net-Pcap-0.17-7.el7.x86_64
t location	(EventID) 45.33.24.242->/var/log/messages
t log_details	Installed: perl-Net-Pcap-0.17-7.el7.x86_64
t ossec_server	OctopusLiveDemo
t path	/var/ossec/logs/alerts/alerts.json
t rule.comment	New Yum package installed.
# rule.level	7
# rule.sidid	2,932
t syslog_host	eventidlabs
t syslog_program	yum[26813]
t syslog_timestamp	May 13 01:24:40
t type	ossec

Facilitando a análise ...

```
[root@eventidlabs ~]# ausearch -k clavis_labs -i -p 26813
----
type=PROCTITLE msg=audit(05/13/16 01:24:29.518:924386) : proctitle=/usr/bin/python /usr/bi
n/yum install perl-Net-Pcap.x86_64
type=PATH msg=audit(05/13/16 01:24:29.518:924386) : item=2 name=/lib64/ld-linux-x86-64.so.
2 inode=13486 dev=08:00 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL
type=PATH msg=audit(05/13/16 01:24:29.518:924386) : item=1 name=/usr/bin/python inode=693
dev=08:00 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL
type=PATH msg=audit(05/13/16 01:24:29.518:924386) : item=0 name=/usr/bin/yum inode=1603 de
v=08:00 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL
type=CWD msg=audit(05/13/16 01:24:29.518:924386) :  cwd=/root
type=EXECVE msg=audit(05/13/16 01:24:29.518:924386) : argc=4 a0=/usr/bin/python a1=/usr/bi
n/yum a2=install a3=perl-Net-Pcap.x86_64
type=SYSCALL msg=audit(05/13/16 01:24:29.518:924386) : arch=x86_64 syscall=execve success=
yes exit=0 a0=0x1638200 a1=0x166f7d0 a2=0x1634480 a3=0x7ffecb3ad860 items=3 ppid=26516 pid
=26813 auid=root uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgi
d=root tty=pts0 ses=3759 comm=yum exe=/usr/bin/python2.7 key=clavis_labs
```

```
[root@eventidlabs ~]# auditctl -l
-a always,exit -F arch=b64 -S listen -F key=backdoor_success
-a always,exit -F arch=b64 -S bind -F success=0 -F key=backdoor_attempt
-a always,exit -F arch=b64 -S execve -F key=clavis_labs
[root@eventidlabs ~]#
```

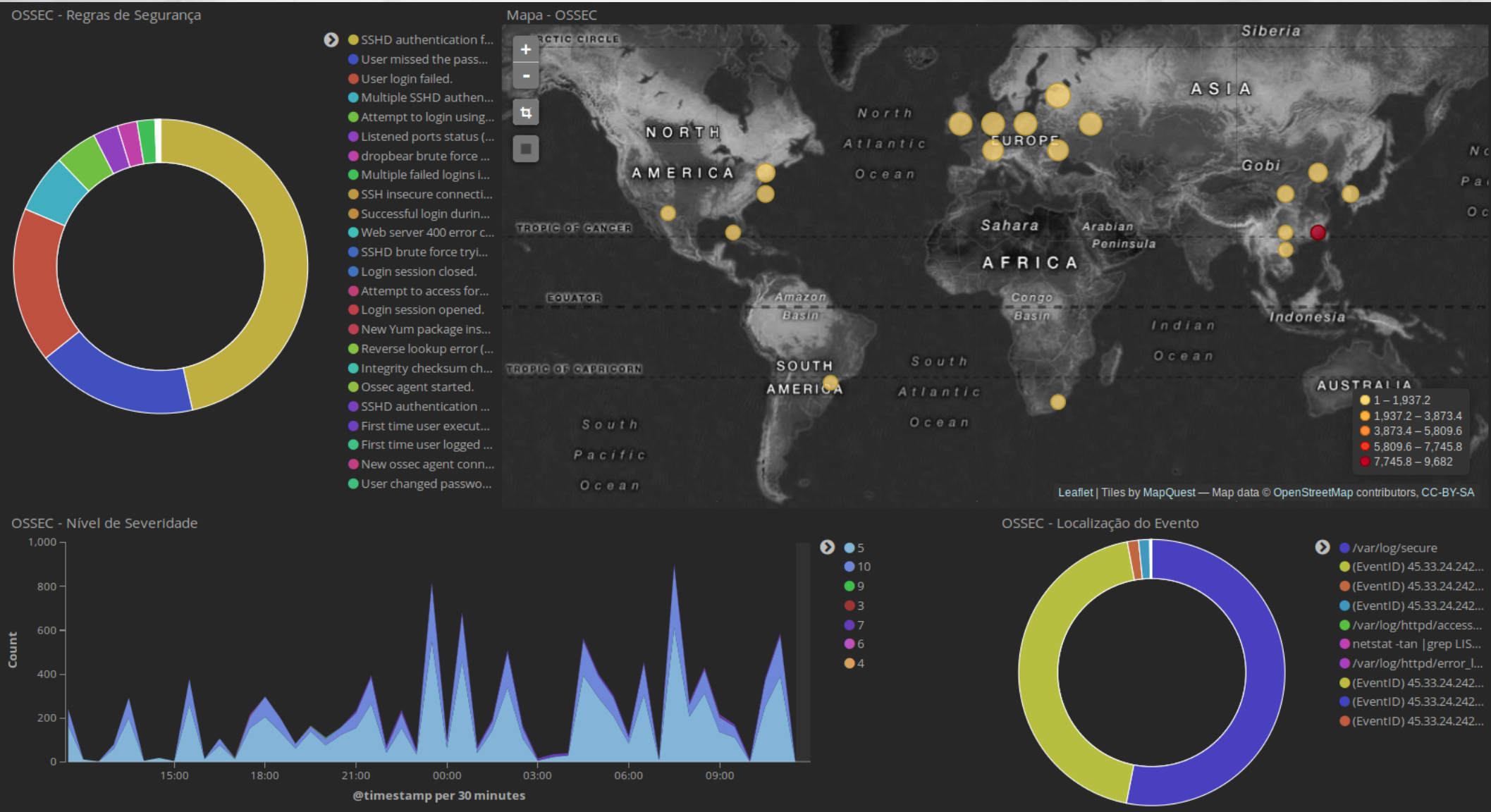
Exemplo alerta (3/3)

Doc: ossec-2016.05.10/ossec/AVSYW_yPbdguFhp0Yk5T

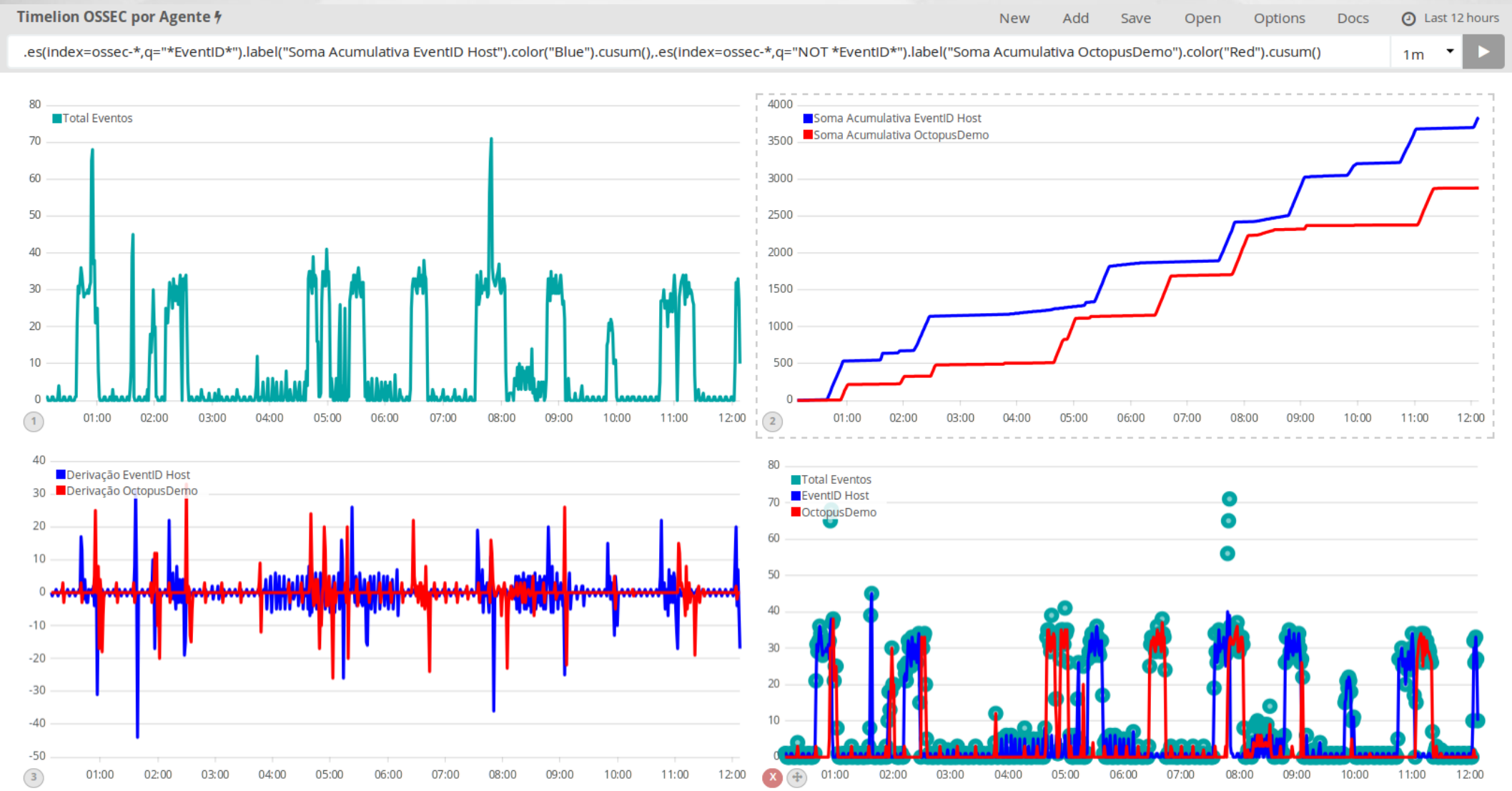
Table | JSON

@timestamp	May 9th 2016, 22:50:45.266
t _id	AVSYW_yPbdguFhp0Yk5T
t _index	ossec-2016.05.10
# _score	1
t _type	ossec
t file.md5_after	e820b98ab599fe4187ad61965cb42bbd
t file.md5_before	a0c83f8bfb62f3e32d6a0ec1d25f515a
t file.path	/etc/shadow
t full_log	Integrity checksum changed for: '/etc/shadow' Old md5sum was: 'a0c83f8bfb62f3e32d6a0ec1d25f515a' New md5sum is : 'e820b98ab599fe4187ad61965cb42bbd' Old sha1sum was: '354b7d503c2d6eb0aa2acf3a42c1ee0e1f33fecf' New sha1sum is : '0d1d8aad5b72a6157d99c543124447fcef9a013e'
t location	(EventID) 45.33.24.242->syscheck
t ossec_server	OctopusLiveDemo
t path	/var/ossec/logs/alerts/alerts.json
t rule.comment	Integrity checksum changed.
# rule.level	7
# rule.sidid	550
t type	ossec

Kibana (vídeo)



Timelion (Vídeo)



Vídeo

Pensando no monitoramento

- O que quero de resposta ?
- O que realmente enviar para o "ELK" ?
- Minha equipe consegue processar os eventos ?
- Contexto

Conclusões / Dicas

- Mapeie a superfície de ataque
- Muita informação crua não te trará melhor resultado
- Entenda plenamente seus logs
- Sempre aprimore o ciclo, as coisas evoluem
- Faça hardening do sistema

Muito Obrigado!

rodrigo@clavis.com.br

@spookerlabs

Rodrigo “Sp0oKeR” Montoro
Pesquisador / Security Operations Center (SOC)