
beclever
.solutions

¿QUIÉN ESTÁ DETRÁS DE BECLEVER SOLUTIONS?

BeClever es una compañía de servicios avanzados en IT que ofrece las soluciones de tecnología de la información más avanzadas

Nuestra misión es ofrecer soluciones tecnológicas innovadoras y de valor que permitan a nuestros clientes cumplir sus objetivos empresariales y ayudarles a alinear sus aplicaciones e infraestructuras tecnológicas con el negocio.

BeClever ofrece las soluciones de tecnología de la información (IT) más avanzadas para clientes del sector público y privado en toda la región EMEA (Europa, Oriente Medio y África). Brindamos una amplia experiencia en las principales compañías de la región, con un equipo humano experto e innovador con el objetivo final de dar el servicio más profesional a nuestros clientes.

Los servicios de BeClever **incluyen consultoría, implantación y gestión de soluciones en las áreas de infraestructura y aplicaciones, gestión de datos y Ciberseguridad.** Adicionalmente, BeClever ofrece ciertos Servicios Cloud para dar solución a las necesidades más recurrentes de nuestros clientes.

TE PRESENTAMOS AL EQUIPO

Luis Alonso
Administración de sistemas Unix/Linux

Luis es experto en administracion de sistemas Unix/Linux y forma parte del equipo de ciberseguridad de BeClever. Se encarga de ayudar a nuestros clientes a facilitar la gestion de sus infraestructuras, securizar y auditar los accesos a los sistemas y gestionar los privilegios de forma adecuada.

Jon Ander
Administración de sistemas

Jon Ander es experto en administracion de sistemas y forma parte del equipo de infraestructura de BeClever. Se encarga de ayudar a nuestros clientes a facilitar la gestion de sus infraestructuras, optimizar el rendimiento de los mismos y garantizar los procesos de backup y recovery de toda la infraestructura.

Mamen Marco Canal
Responsable del área de Gestión de Datos

Con gran expertise en administración, tuning y replicación de BBDD. Mamen es la responsable del área de gestión de datos de BeClever, donde ayudamos a nuestros clientes a mejorar la eficiencia de sus procesos relacionados con bbdd, migraciones, etc..

Joxan Crego Muñoz
Senior Consultant

Joxan es experto en administración de soluciones Microsoft y forma parte del equipo de ciberseguridad de BeClever. Se encarga de ayudar a nuestros clientes a facilitar la gestion de sus infraestructuras, securizar y auditar los accesos a los sistemas y gestionar los privilegios de forma adecuada.

Javi Sáenz López
Senior Consultant

Javi tiene una amplia experiencia en proyectos de Business Inteligence, desarrollo en sql y pl/sql, tuning de bbdd y optimización de queries, ejecutando los principales proyectos en esta materia en nuestros clientes.

Edurne Amor San Miguel
Account Manager

Edurne se encarga de la gestión diaria de la relación con nuestros clientes y proveedores, incluyendo la presentacion, definición, seguimiento y gestión de propuestas, así como de la interlocución con los proveedores.

David Fernández Pagés
Senior Consultant

David es experto en administracion de soluciones Microsoft y forma parte del equipo de ciberseguridad de BeClever. Se encarga de ayudar a nuestros clientes a facilitar la gestion de sus infraestructuras, securizar y auditar los accesos a los sistemas y gestionar los privilegios de forma adecuada.

David Fernández Benito
CTO y fundador de BeClever

David, experto en soluciones de seguridad y gestión de identidades, es el responsable del área de Ciberseguridad de BeClever, donde ayudamos a nuestros clientes a gestionar de una manera más eficiente los permisos y accesos de sus empleados y usuarios.

Alvaro Moreno Guerra
Technical Account Manager

Alvaro ha ejercido durante años labores de consultor en proyectos de infraestructura y monitorización, habiendo pasado a responsabilizarse de la relación comercial con nuestros clientes.

Aiert Azueta Dudagoitia
CEO y fundador de BeClever

Con una capacidad importante para entender las necesidades de los clientes y analizar las nuevas soluciones que el mercado ofrece, Aiert se dedica a definir y ofrecer los servicios necesarios que nuestros clientes buscan para mejorar su productividad y alinear las necesidades de negocio con las infraestructuras IT, así como a definir las alianzas con fabricantes de software y otras compañías de servicios IT.

En un entorno donde la seguridad es cada vez más importante, debemos disponer de los métodos más avanzados para detectar y prevenir los posibles ataques a nuestras organizaciones.
Los métodos de ataque han cambiado en los últimos años, pasando de ataques dirigidos a ataques indiscriminados, donde cualquiera puede ser objetivo de los ciberdelincuentes. Los métodos tradicionales de seguridad, por si mismos, ya no son suficientes, y debemos complementarlos con otras medidas de seguridad más avanzadas.

Desde BeClever, le ayudaremos a complementar las medidas tradicionales con las medidas más avanzadas en ciberseguridad, de forma que pueda minimizar los riesgos y superficie de ataque.

El punto más vulnerable de todas nuestras organizaciones son los propios empleados y usuarios de las compañías, que, con el simple hecho de pulsar un link en un mail, pueden llegar a comprometer toda la información de la compañía.
Además, las nuevas normas, regulaciones, y leyes, como puede ser la nueva RGPD (Regulación General de Protección de Datos) o GDPR (General Data Protection Regulation) por sus siglas en inglés, de la Unión Europea, nos obligan a aumentar las medidas de seguridad de datos de carácter personal.

Existen dos tipos de usuarios en cualquier compañía, **los usuarios con permisos normales, y los usuarios con permisos de administrador.** Evidentemente, el riesgo de los segundos es muy superior al de los primeros, aunque en un ciberataque, los ciberdelincuentes pueden escalar su nivel de privilegios desde usuarios normales hasta administradores, cuando podrán explotar a su antojo toda la información de la compañía.
Para proteger los permisos de los usuarios, desde BeClever **apostamos por soluciones de Gestión de Identidad (IAM-Identity and Access Management)**, que permitirán a las compañías realizar una gestión efectiva de los permisos de los usuarios, basado en roles, automatizando el aprovisionamiento y deaprovisionamiento y las operaciones de alta/baja/modificación de los usuarios. Para la gestión de accesos, proveemos soluciones de Single Sign-On y soluciones de doble Factor de Autenticación.

Las soluciones de Gestión de Cuentas Privilegiadas o PAM (Privileged Access Management), nos permitirán securizar los accesos de los usuarios administradores con accesos privilegiados, evitando que estos usuarios dispongan de las contraseñas que permitan a los ciberdelincuentes explotar las vulnerabilidades más graves.

Además, cubriremos otros aspectos de seguridad como auditoria de accesos y permisos, análisis de vulnerabilidades, delegación de permisos, enmascaramiento de datos, etc..

NUESTROS PARTNERS TECNOLÓGICOS

Nuestro objetivo principal es el de convertirnos en el socio tecnológico de nuestros clientes, y ello implica asumir responsabilidades y garantizar el compromiso de proporcionar soluciones de calidad, avaladas por el know-how de expertos profesionales. Nuestro nivel de Partnership con los principales fabricantes de Software y Hardware nos distingue en el mercado añadiendo valor a todos nuestros proyectos.

actifio · APPDYNAMICS · Bitdefender · CITRIX · CYBERARK · informatica · Microsoft · NetApp · ONE IDENTITY · optimyth · ORACLE · Quest · Symantec · VEEAM · VERITAS · vmware · wanDISCO · NAKIVO Backup & Replication

¿QUIERES MÁS INFORMACIÓN?

Escribe y tu email y te contactaremos

ENVIAR

Acepto el almacenamiento y gestión de mis datos por parte de esta web

Acepto las condiciones de privacidad

+34 946073341

info@beclever.solutions

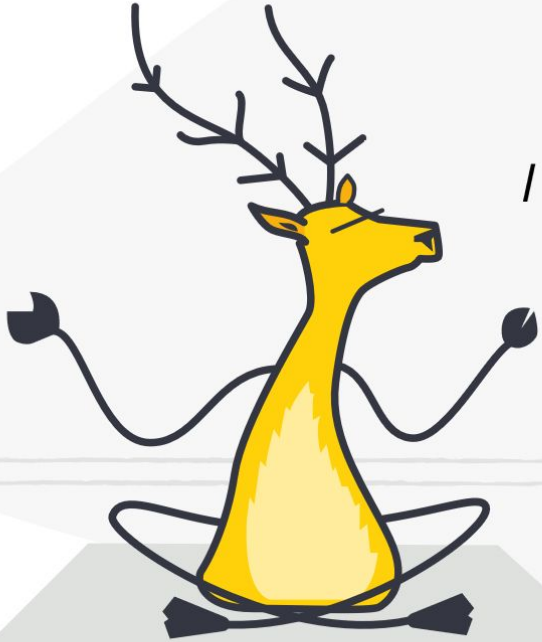
beclever .solutions

LOCALIZACIÓN

Carretera Bilbao-Galdakao 10
(Bolueta)
2º planta, Módulos 2 y 3
Bilbao – 48004

+34 946073341
info@beclever.solutions

SÍGUENOS EN REDES



I am one with the Elastic Stack.

Get to know the real ELK Stack.

elastic


ELK
Stack


elastic
logstash
kibana

Elastic Stack

- **ElasticSearch** https://www.elastic.co/products/elasticsearch Motor de búsqueda y análisis de texto completo donde se almacenan datos ya optimizados por la indexación. Distribuido, escalable, tolerante a fallos y alta disponibilidad.
- **Logstash** https://www.elastic.co/products/logstash Para recopilar registros de diferentes fuentes, analizarlos y almacenarlos para su uso posterior.
- **Kibana** https://www.elastic.co/products/kibana es un cuadro de mandos o tablero de visualización flexible e intuitivo para la monitorización. https://www.elastic.co/guide/en/kibana/current/index.html

Elastic Stack

https://www.elastic.co/es/elk-stack

https://www.elastic.co/guide/index.html

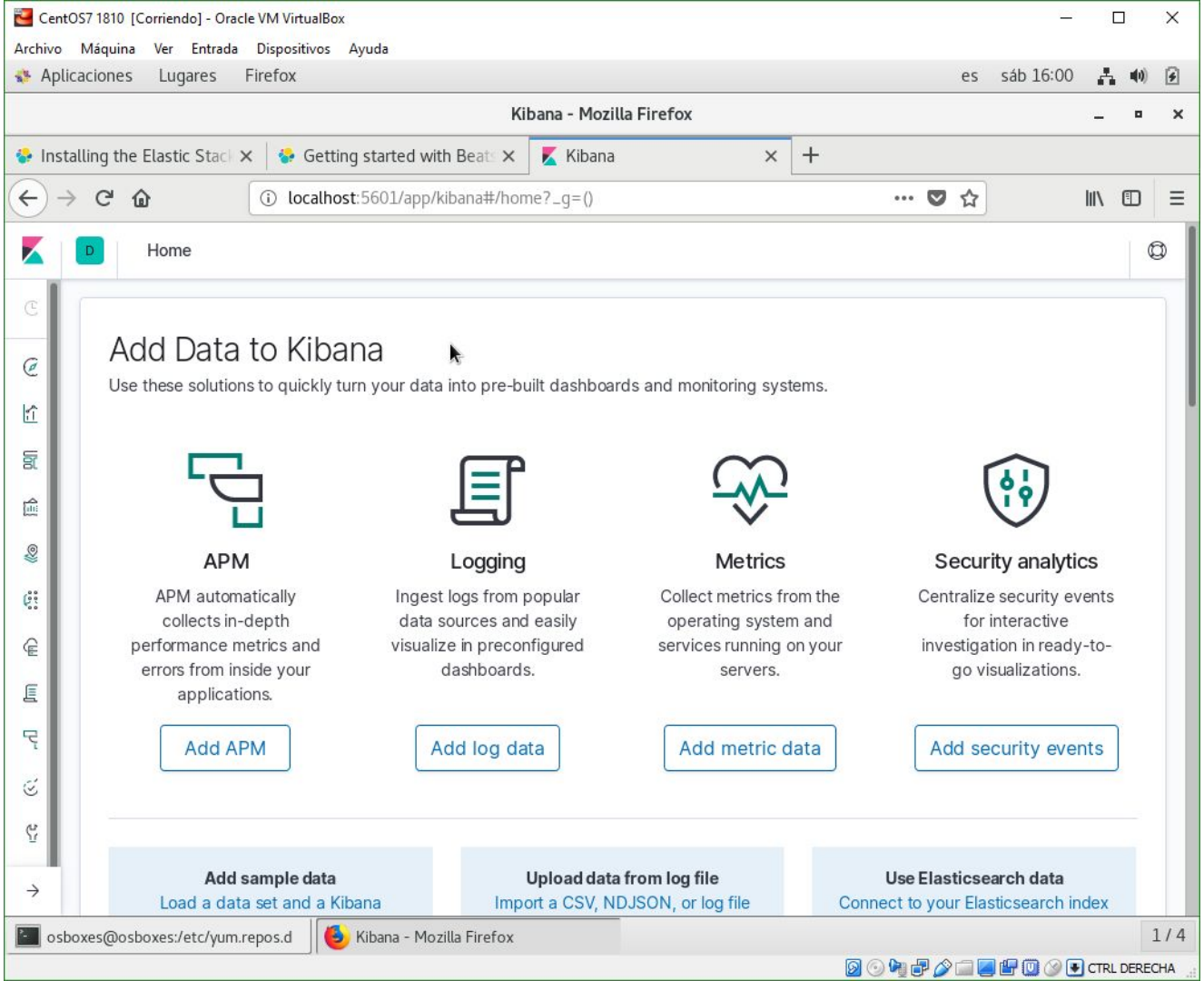
https://www.elastic.co/guide/en/elasticsearch/reference/7.0/install-elasticsearch.html

https://www.elastic.co/guide/en/elasticsearch/reference/7.0/rpm.html

https://www.elastic.co/es/start

Orden de instalación para productos Elastic Stack:

1. Elasticsearch https://www.elastic.co/guide/en/elasticsearch/reference/7.0/install-elasticsearch.html
2. Kibana https://www.elastic.co/guide/en/kibana/7.0/install.html
3. Logstash http://www.elastic.co/guide/en/logstash/7.0/installing-logstash.html
4. Beats https://www.elastic.co/guide/en/beats/libbeat/7.0/getting-started.html
5. APM Server https://www.elastic.co/guide/en/apm/server/7.0/installing.html


CentOS7 1810 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares Firefox
es sáb 16:00
Kibana - Mozilla Firefox
Installing the Elastic Stack
Getting started with Beats
Kibana
localhost:5601/app/kibana#/home?_g=()
Home
Add Data to Kibana
Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.
APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
Add APM
Logging
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
Add log data
Metrics
Collect metrics from the operating system and services running on your servers.
Add metric data
Security analytics
Centralize security events for interactive investigation in ready-to-go visualizations.
Add security events
Add sample data
Load a data set and a Kibana
Upload data from log file
Import a CSV, NDJSON, or log file
Use Elasticsearch data
Connect to your Elasticsearch index
osboxes@osboxes:/etc/yum.repos.d
Kibana - Mozilla Firefox
1 / 4
CTRL DERECHA

CentOS7 1810 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Aplicaciones Lugares Firefox es sáb 16:22

Kibana - Mozilla Firefox

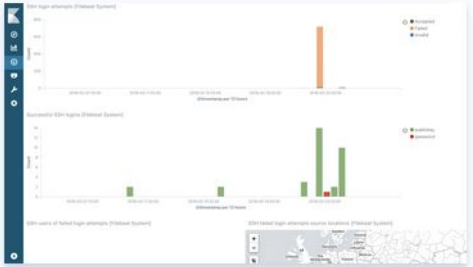
Installing the Elastic Stack | Getting started with Beats | Kibana

localhost:5601/app/kibana#/home/tutorial/systemLogs?_g=()

Home / Add data / System logs

System logs

The `system` Filebeat module collects and parses logs created by the system logging service of common Unix/Linux based distributions. This module is not available on Windows. Learn more.



View exported fields

Self managed | Elastic Cloud

Getting Started

macOS DEB RPM

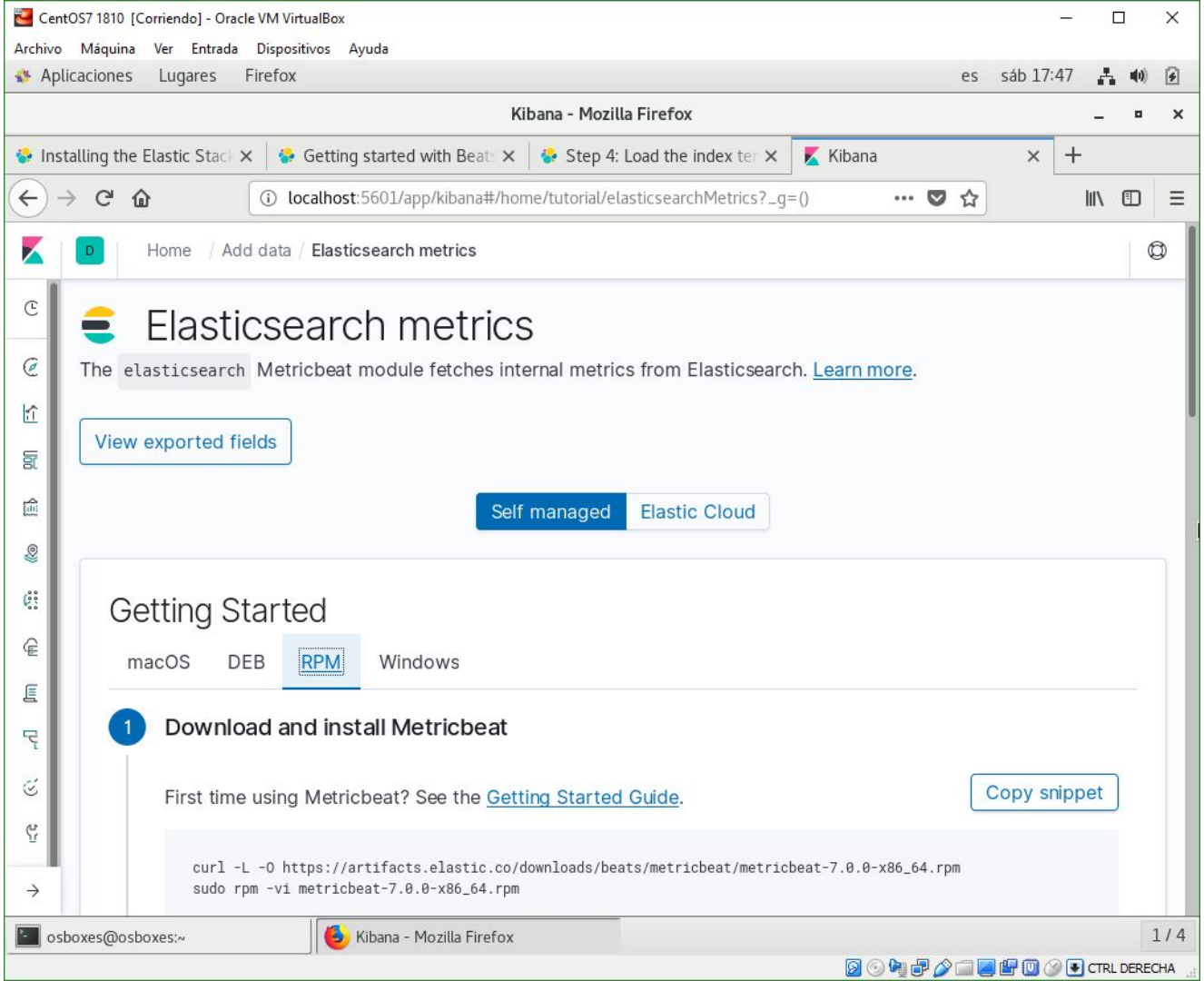
1 Download and install Filebeat

First time using Filebeat? See the Getting Started Guide.

Copy snippet

osboxes@osboxes:/etc/yum.repos.d | Kibana - Mozilla Firefox | 1 / 4

CTRL DERECHA

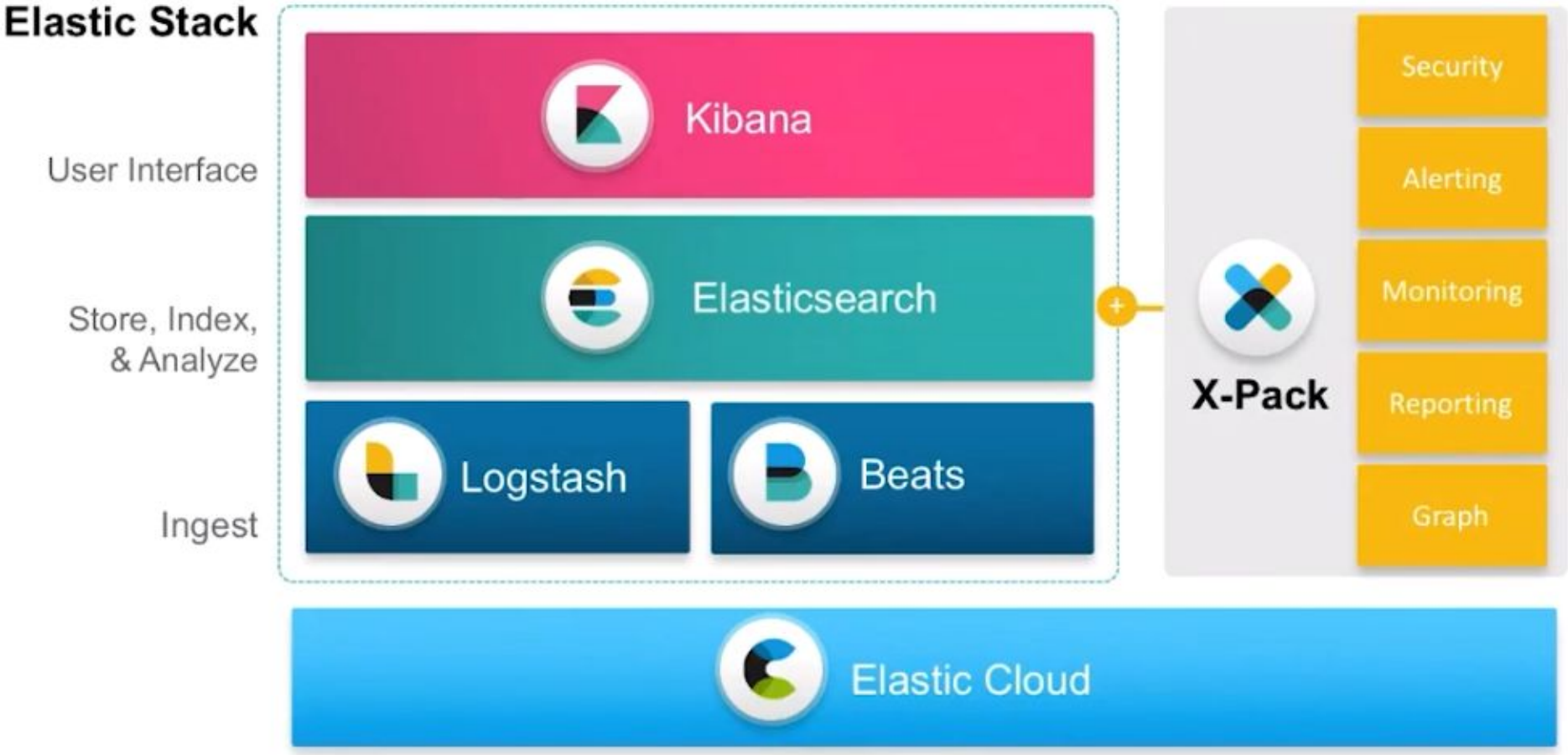

CentOS7 1810 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares Firefox
es sáb 17:47
Kibana - Mozilla Firefox
Installing the Elastic Stack
Getting started with Beats
Step 4: Load the index ter
Kibana
localhost:5601/app/kibana#/home/tutorial/elasticsearchMetrics?_g=()
Home / Add data / Elasticsearch metrics
Elasticsearch metrics
The elasticsearch Metricbeat module fetches internal metrics from Elasticsearch. Learn more.
View exported fields
Self managed
Elastic Cloud
Getting Started
macOS
DEB
RPM
Windows
1
Download and install Metricbeat
First time using Metricbeat? See the Getting Started Guide.
Copy snippet
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.0.0-x86_64.rpm
sudo rpm -vi metricbeat-7.0.0-x86_64.rpm
osboxes@osboxes:~
Kibana - Mozilla Firefox
1 / 4
CTRL DERECHA

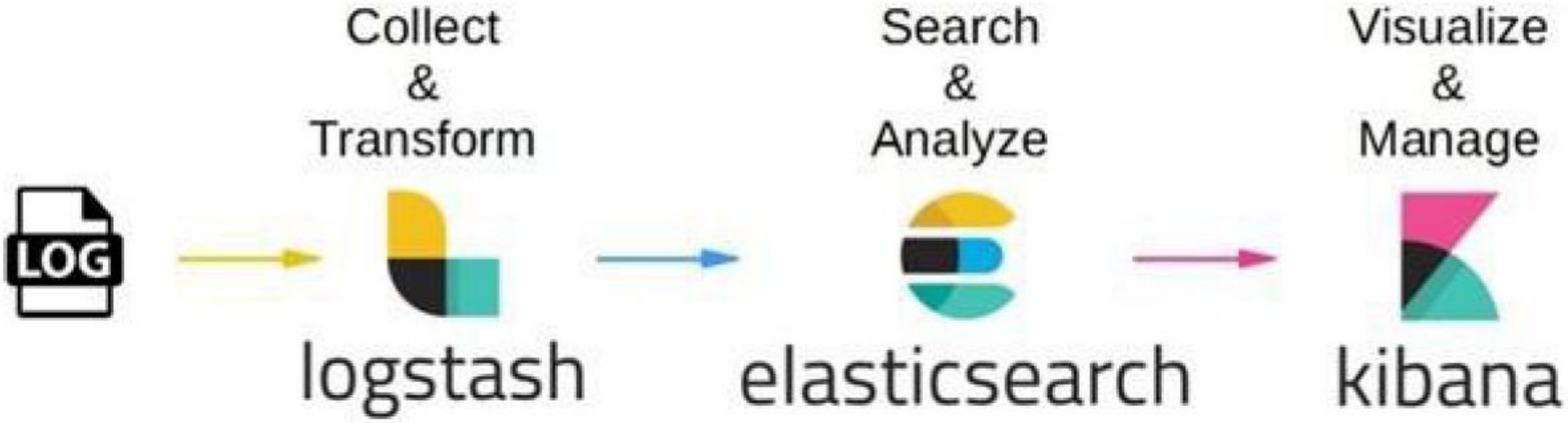
Data Collection

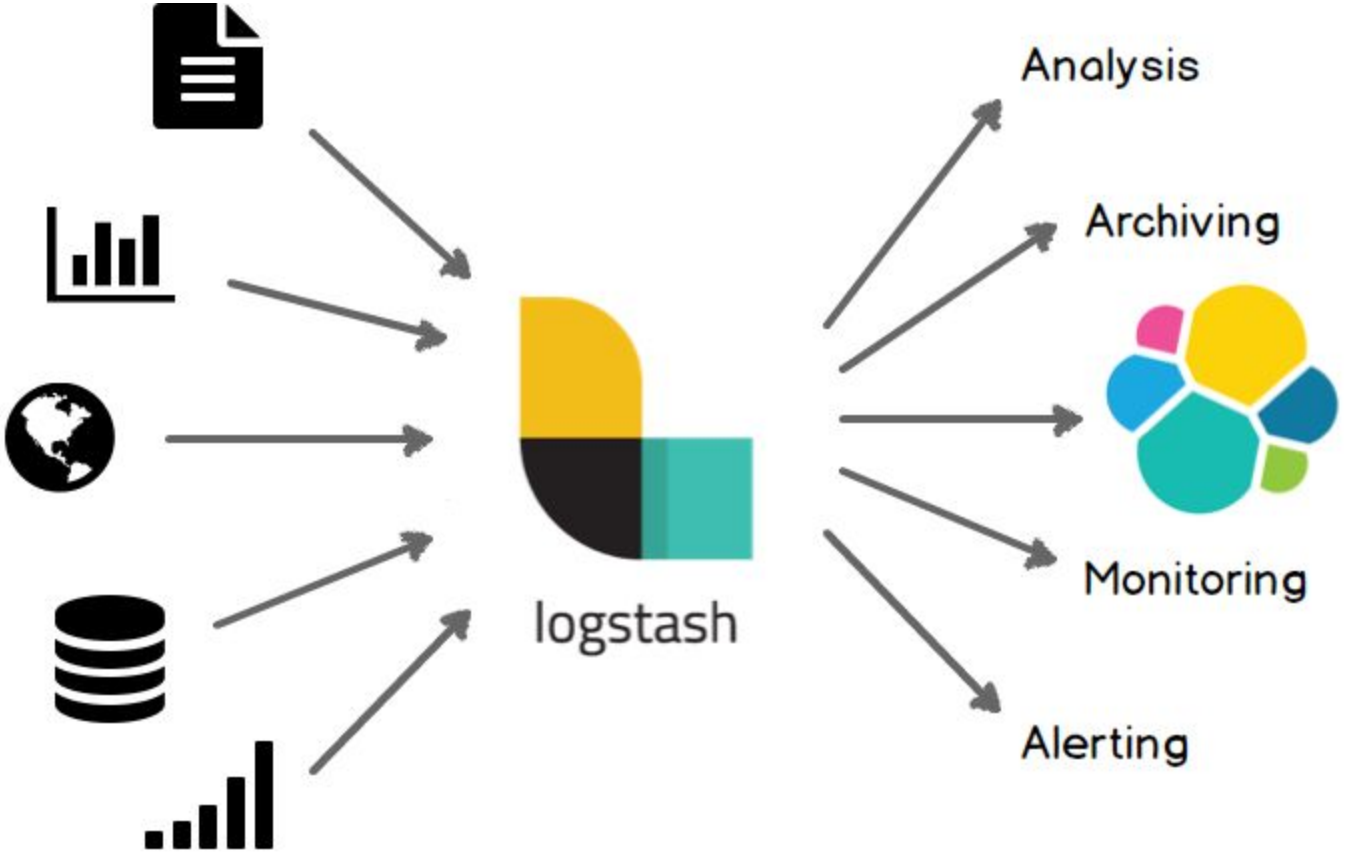
Data Aggregation & Processing

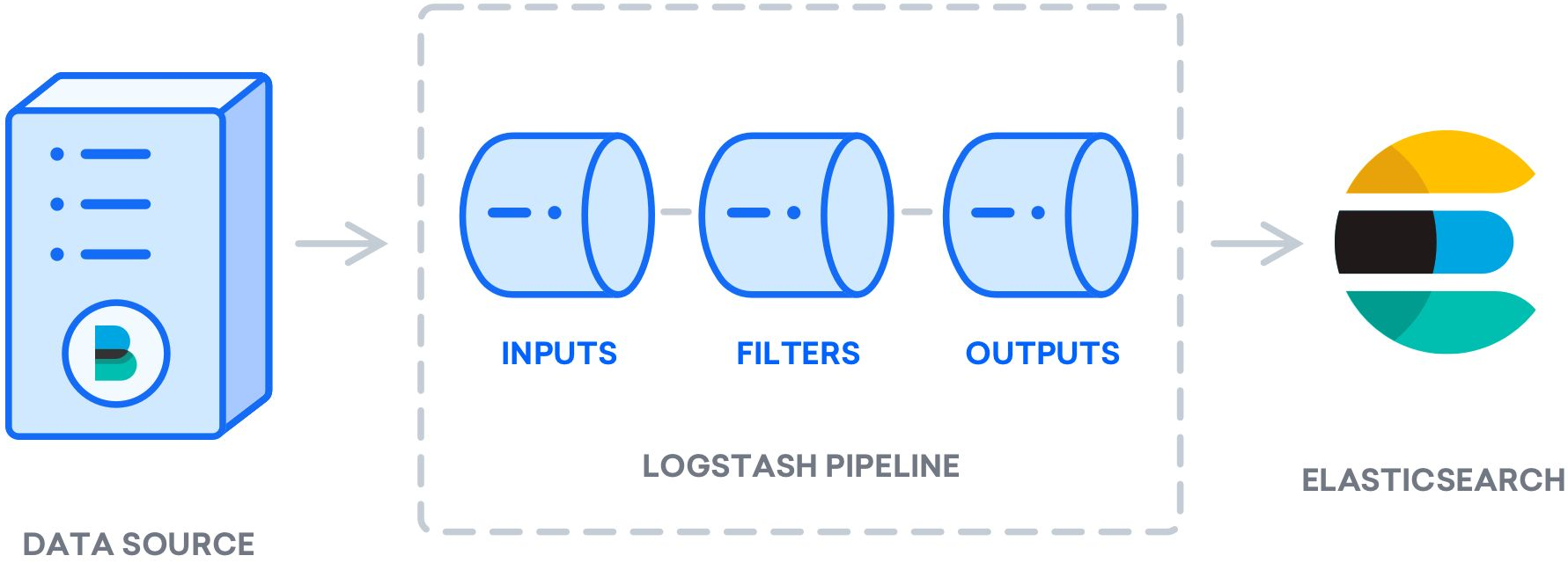
Indexing & storage

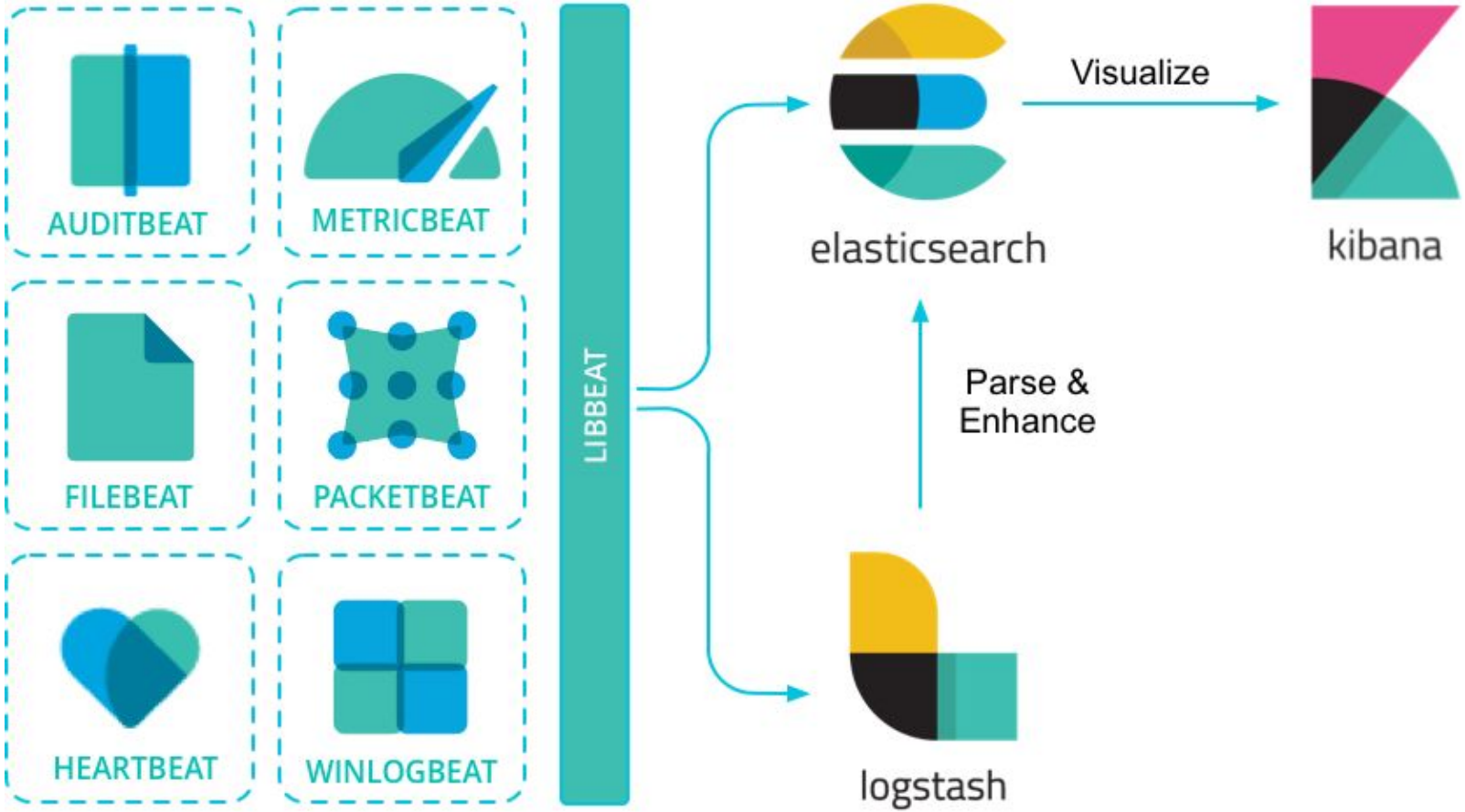
Analysis & visualization

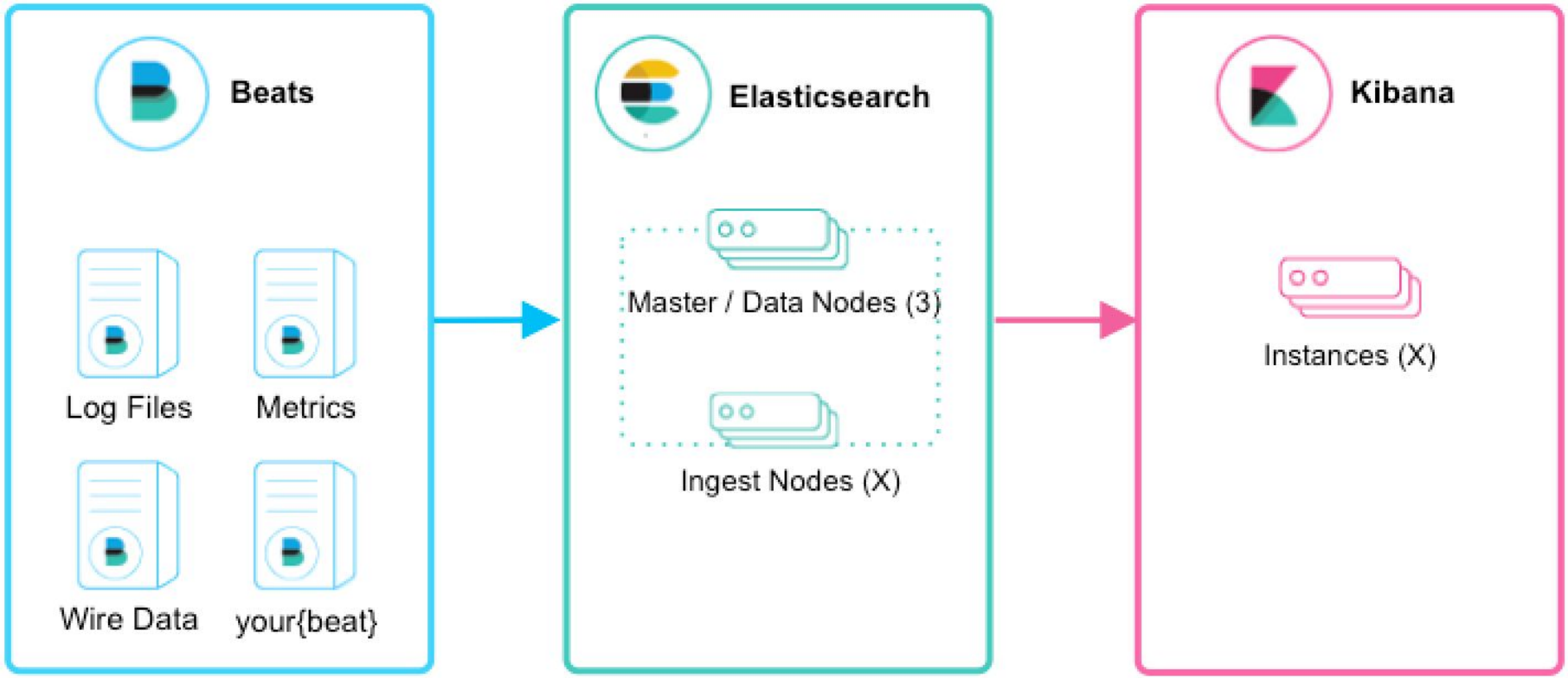

Elastic Stack
User Interface
Store, Index, & Analyze
Ingest
Kibana
Elasticsearch
Logstash
Beats
X-Pack
Security
Alerting
Monitoring
Reporting
Graph
Elastic Cloud


LOG
Collect
&
Transform
logstash
Search
&
Analyze
elasticsearch
Visualize
&
Manage
kibana


Analysis
Archiving
Monitoring
Alerting
logstash


INPUTS
FILTERS
OUTPUTS
LOGSTASH PIPELINE
DATA SOURCE
ELASTICSEARCH


AUDITBEAT
METRICBEAT
FILEBEAT
PACKETBEAT
HEARTBEAT
WINLOGBEAT
LIBBEAT
elasticsearch
Visualize
kibana
Parse &
Enhance
logstash


Beats
Log Files
Metrics
Wire Data
your{beat}
Elasticsearch
Master / Data Nodes (3)
Ingest Nodes (X)
Kibana
Instances (X)

https://www.elastic.co/guide/index.html

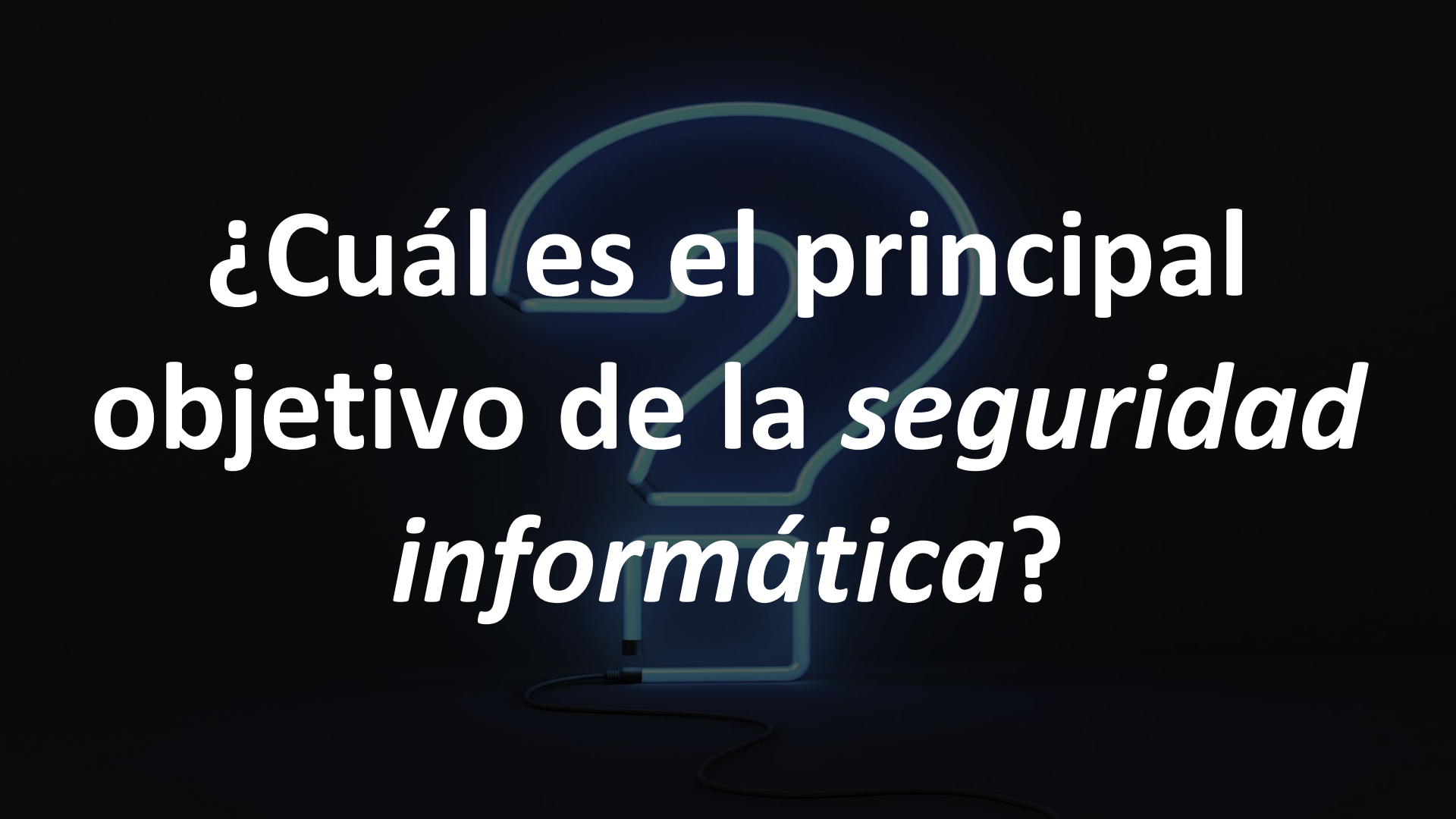
Beats https://www.elastic.co/guide/en/beats/libbeat/7.0/getting-started.html

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

- Audit data https://www.elastic.co/products/beats/auditbeat
- Log files https://www.elastic.co/products/beats/filebeat
- Availability https://www.elastic.co/products/beats/heartbeat
- Metrics https://www.elastic.co/products/beats/metricbeat
- Network traffic https://www.elastic.co/products/beats/packetbeat
- Windows event logs https://www.elastic.co/products/beats/winlogbeat
- https://www.elastic.co/guide/en/beats/libbeat/current/community-beats.html

Extracción de datos de los registros de logs para su envío y centralización.

- **Filebeat**
  - https://www.elastic.co/products/beats/filebeat
  - https://www.elastic.co/guide/en/beats/filebeat/current/index.html
  - https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-getting-started.html
  - https://github.com/elastic/beats/tree/master/filebeat


¿Cuál es el principal objetivo de la *seguridad informática*?

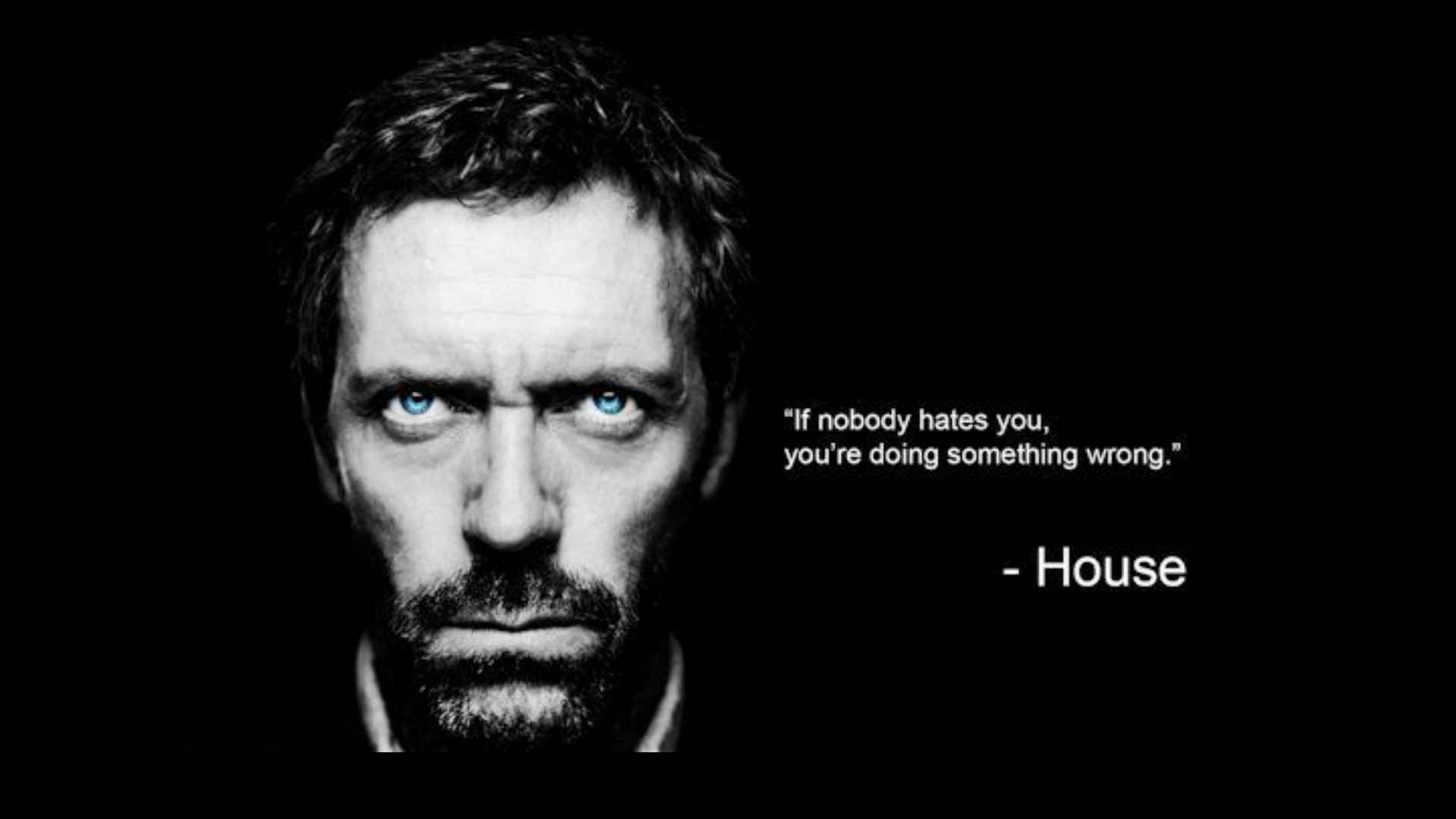
El objetivo de la seguridad informática es:

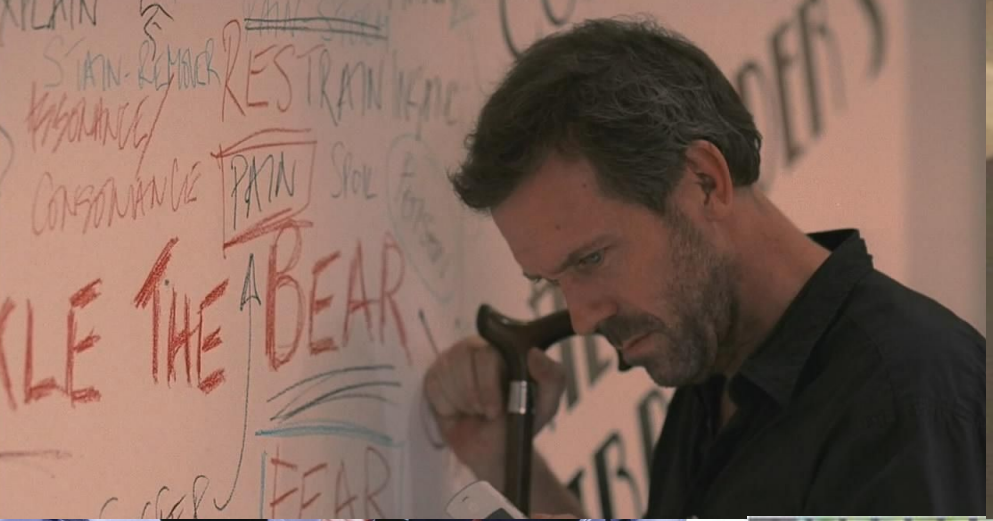
- Proteger el **principal activo** de cualquier organización.

La información

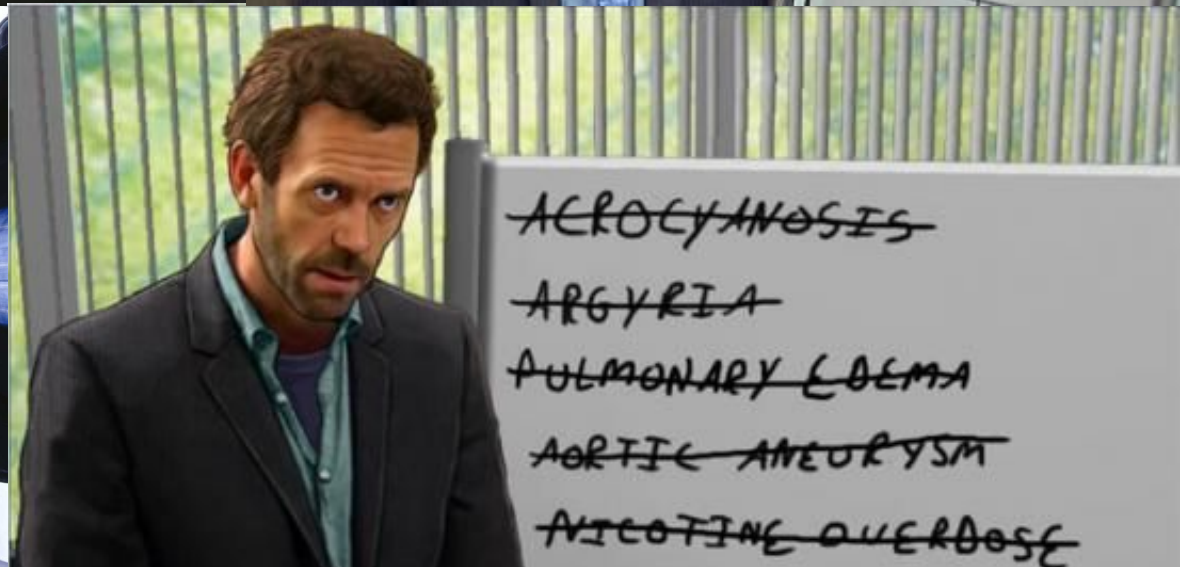

El proceso productivo

Infraestructuras críticas

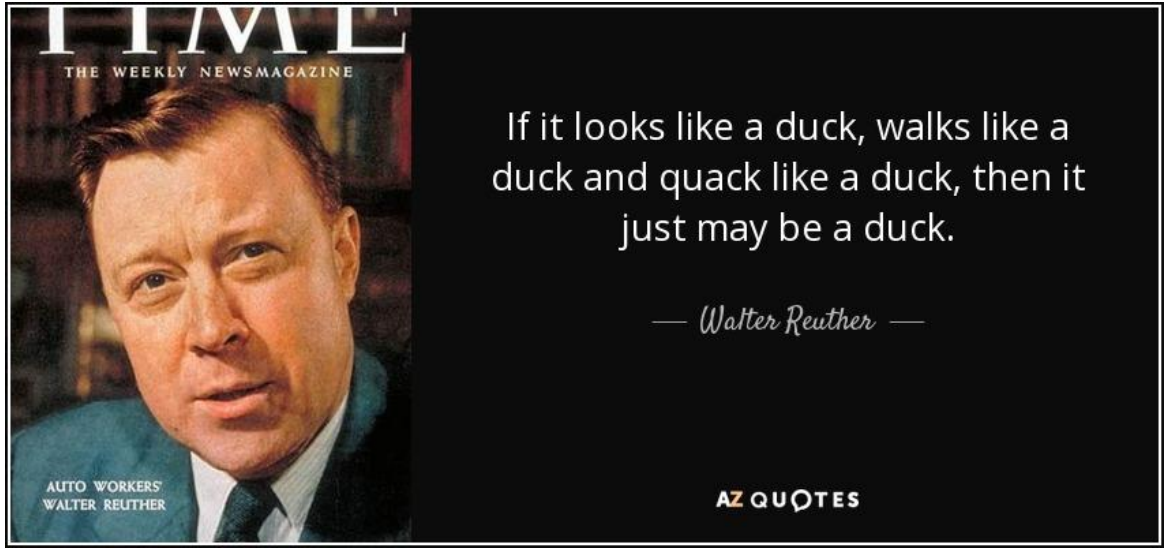

"If nobody hates you,
you're doing something wrong."
- House


RESTRAIN
PAIN
THE
BEAR

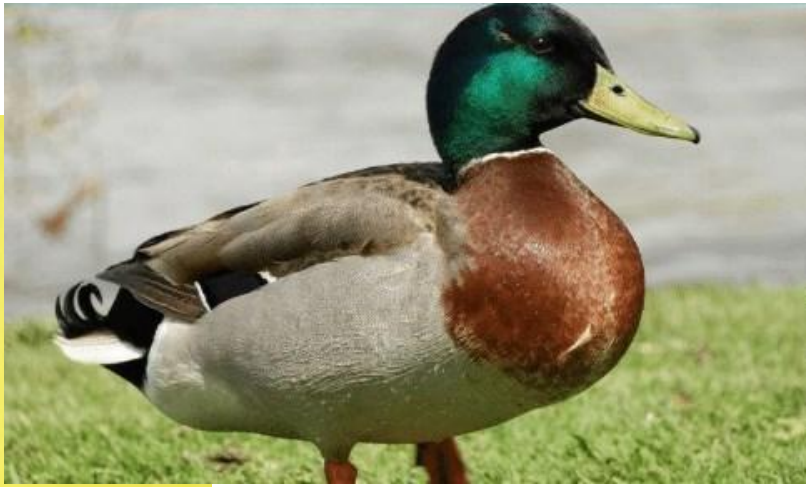

"DEAD MAN DYING"
SYMPTOMS
CAUSES


ACROCYANOSIS
ARGYRIA
PULMONARY EDEMA
AORTIC ANEURYSM
NICOTINE OVERDOSE

- *It’s a duck...*

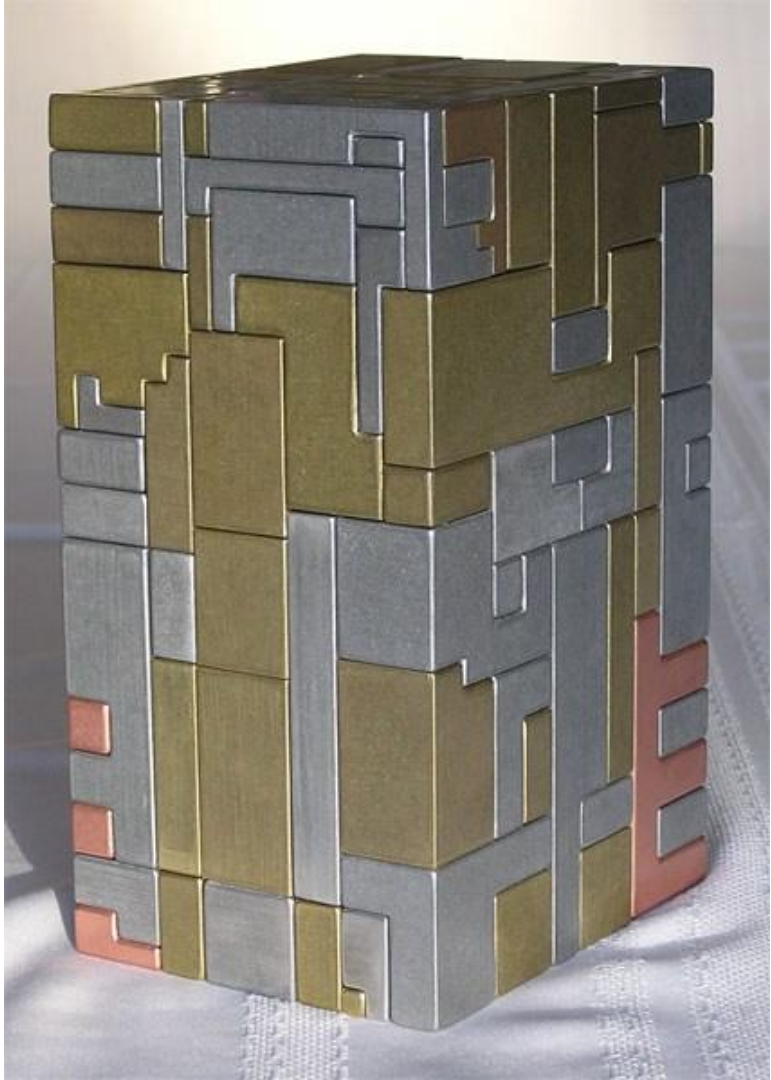

TIME
THE WEEKLY NEWSMAGAZINE
AUTO WORKERS'
WALTER REUTHER
If it looks like a duck, walks like a duck and quack like a duck, then it just may be a duck.
— Walter Reuther —
AZ QUOTES

- *… or NOT.*




- No lo sé Rick, parece falso...

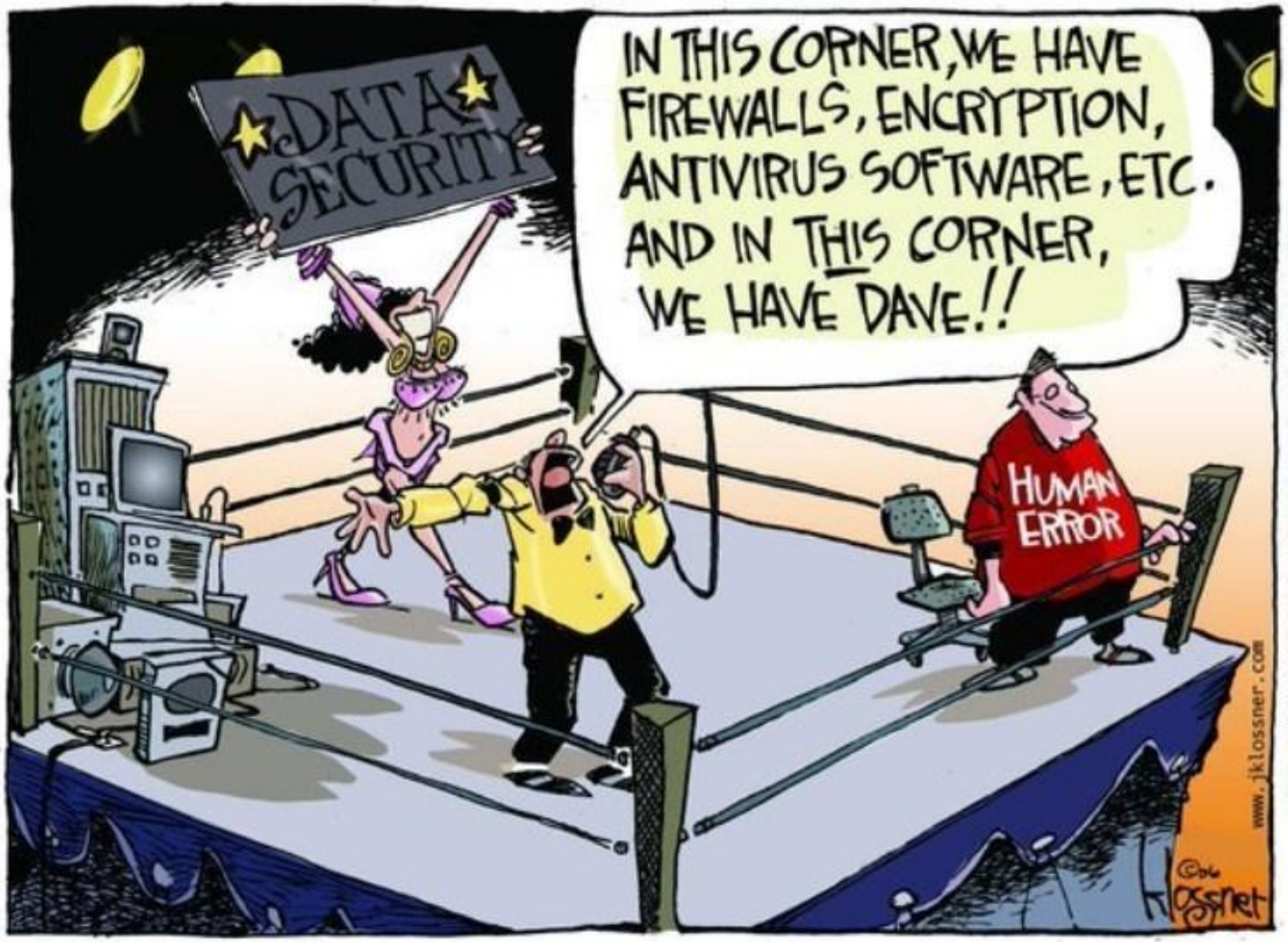
- *¿Puede este objeto suponer una* ***amenaza****?*



- *Vamos a analizarlo:*

- *Montando las piezas adecuadas del modo adecuado...*


It's yellow, it's ugly, it doesn't match anything,
but it can save lives.
Safety vest and reflective triangle will be obligatory in every vehicle. Get equipped now.
ROAD SAFETY
WE ARE ALL RESPONSIBLE



copyright 2006 john klossner, www.jklossner.com

FortiClient

FORTINET

FortiClient for Linux

Expanded FortiClient Endpoint protection and attack surface coverage.

LEARN MORE

DOWNLOAD

Next Generation Endpoint Protection

Free Downloads

Get FortiClient 6.0 for Windows
Windows 7 or higher supported
Download

Get FortiClient 6.0 for Mac OSX
Mac OSX v10.12 Sierra or higher

Get FortiClient 6.0 for Linux
Ubuntu 16.04 or higher
Red Hat, CentOS 7.4 or higher

Get FortiClient for iOS
iOS 9.0.0 or higher

Get FortiClient for Android
Android 4.1 or higher

Get FortiClient App for Windows
Windows 10 and Windows Phone 10

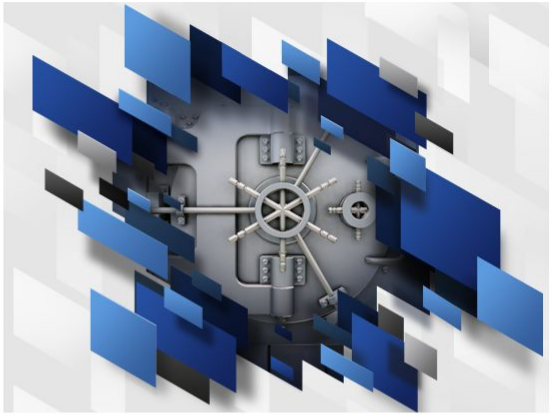
Get FortiClient for Chromebook
Google Chromebook and Chrome Browser

FortiClient for Windows

- AntiVirus
- SSL-VPN
- Security Fabric Telemetry
- Compliance Enforcement
- Web Filtering
- IPSec VPN
- Application Firewall
- 2-Factor Authentication
- Vulnerability Scan
- WAN Optimization
- On-net detection for auto-VPN
- Rebranding
- Anti-Exploit

Technical Specification

CYBERARK | Privileged Access Security

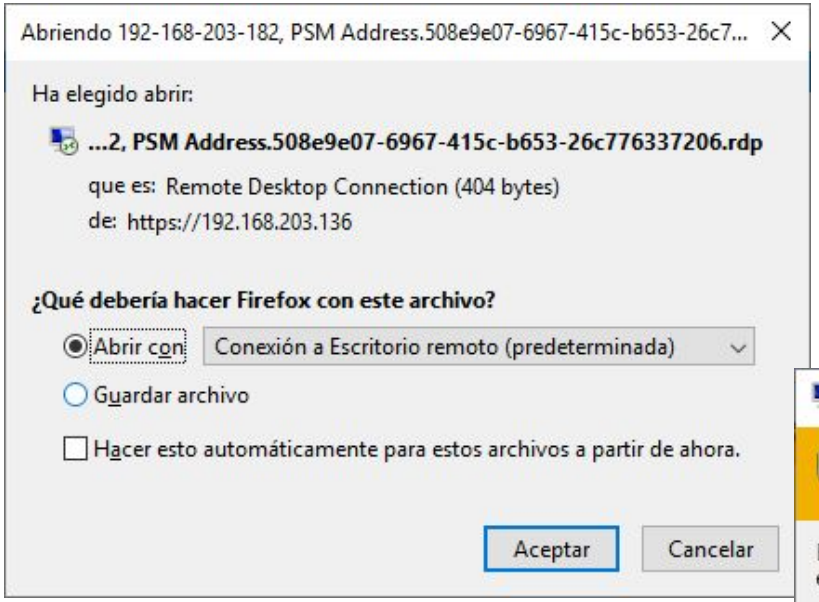


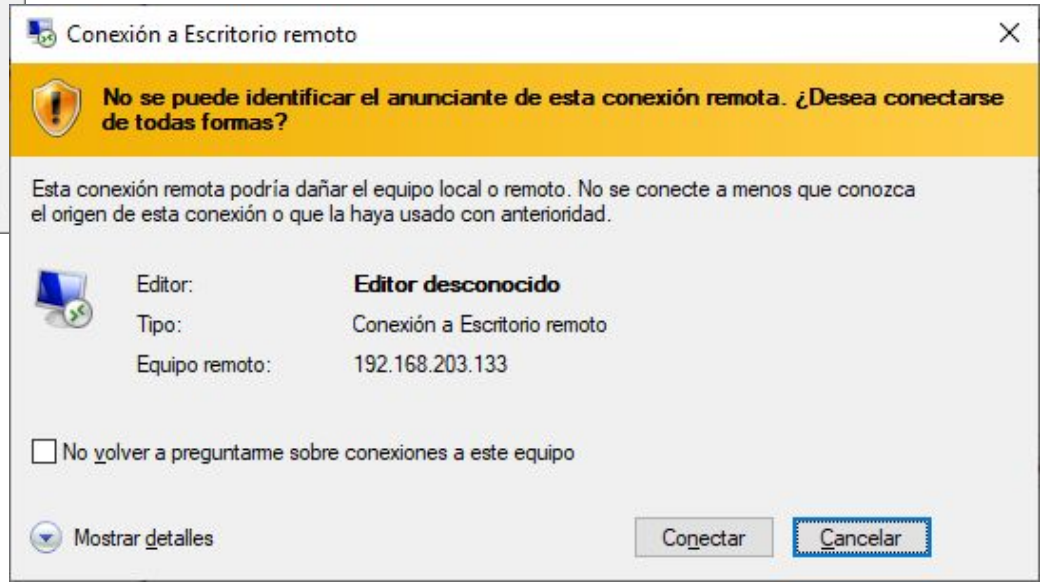
SIGN IN

Please choose an authentication method

CyberArk | LDAP

Copyright © 1999-2018 CyberArk Software Ltd. All Rights Reserved.
Version 10.5.0 (10.5.0.48) About | Mobile version


Abriendo 192-168-203-182, PSM Address.508e9e07-6967-415c-b653-26c7...
Ha elegido abrir:
...2, PSM Address.508e9e07-6967-415c-b653-26c776337206.rdp
que es: Remote Desktop Connection (404 bytes)
de: https://192.168.203.136
¿Qué debería hacer Firefox con este archivo?
Abrir con
Conexión a Escritorio remoto (predeterminada)
Guardar archivo
Hacer esto automáticamente para estos archivos a partir de ahora.
Aceptar
Cancelar


Conexión a Escritorio remoto
No se puede identificar el anunciante de esta conexión remota. ¿Desea conectarse de todas formas?
Esta conexión remota podría dañar el equipo local o remoto. No se conecte a menos que conozca el origen de esta conexión o que la haya usado con anterioridad.
Editor:
Editor desconocido
Tipo:
Conexión a Escritorio remoto
Equipo remoto:
192.168.203.133
No volver a preguntarme sobre conexiones a este equipo
Mostrar detalles
Conectar
Cancelar

The CentOS Project

The CentOS Project is a community-driven free software effort focused on delivering a robust open source ecosystem. For users, we offer a consistent manageable platform that suits a wide variety of deployments. For open source communities, we offer a solid, predictable base to build upon, along with extensive resources to build, test, release, and maintain their code.

We're also expanding the availability of CentOS images across a number of vendors, providing official images for Amazon, Google, and more. For self-hosted cloud, we also provide a generic cloud-init enabled image.

For more information about updates and improvements in CentOS 7, please check out the release notes or the release announcement in the mailing list archive.

Get CentOS Now

OpenJDK http://openjdk.java.net/

https://www.elastic.co/guide/en/elasticsearch/reference/7.0/setup.html#jvm-version

https://www.elastic.co/guide/en/elasticsearch/reference/current/rpm.html

192.168.203.182:5601/app/kibana#/home?_g=()

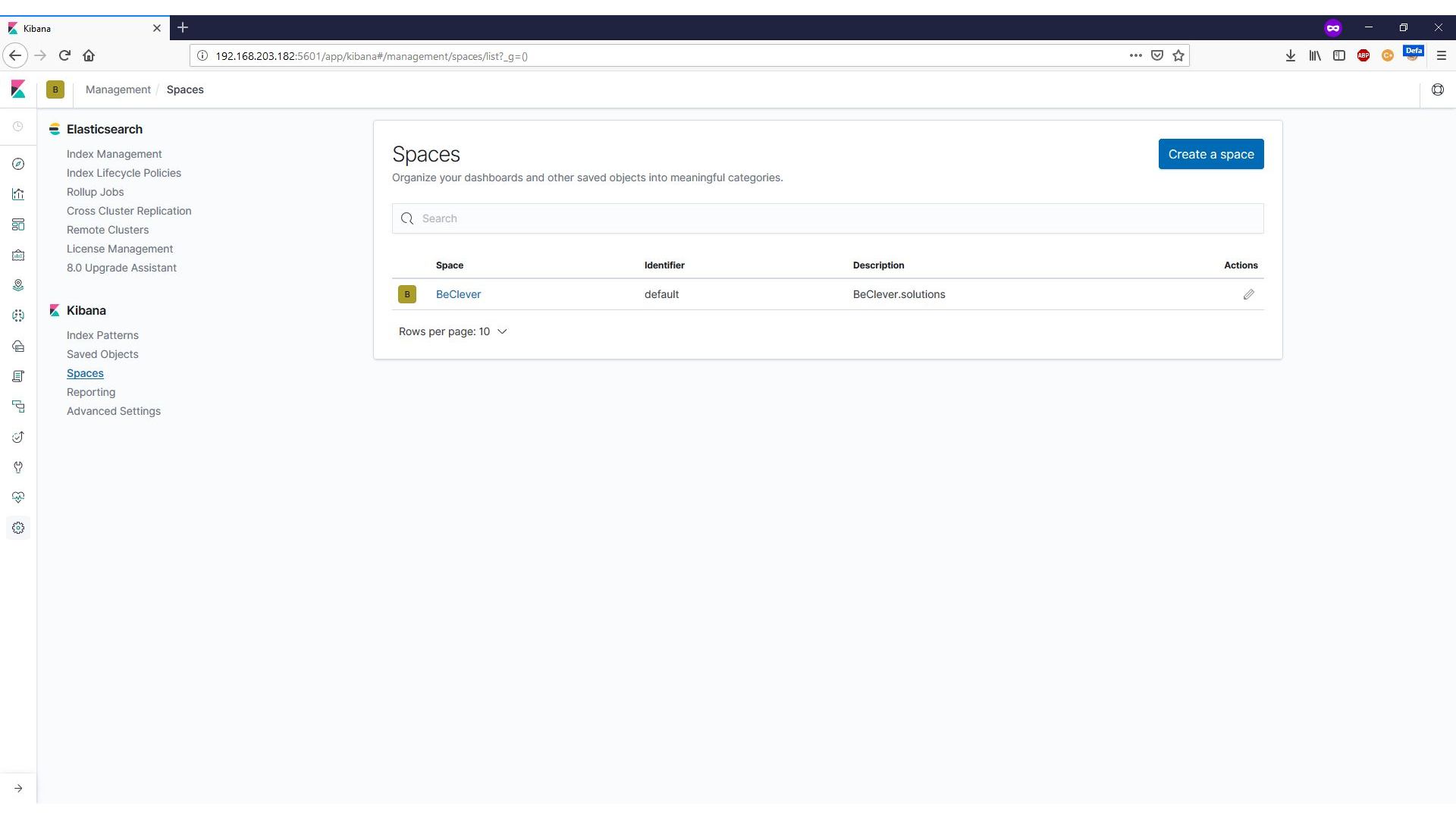
Welcome to Kibana

Your window into the Elastic Stack

Let's get started

We noticed that you don't have any data in your cluster. You can try our sample data and dashboards or jump in with your own data.

Try our sample data Explore on my own


Kibana
192.168.203.182:5601/app/kibana#/management/spaces/list?_g=()
Management / Spaces
Elasticsearch
Index Management
Index Lifecycle Policies
Rollup Jobs
Cross Cluster Replication
Remote Clusters
License Management
8.0 Upgrade Assistant
Kibana
Index Patterns
Saved Objects
Spaces
Reporting
Advanced Settings
Spaces
Organize your dashboards and other saved objects into meaningful categories.
Create a space
Search
Space
Identifier
Description
Actions
B
BeClever
default
BeClever.solutions
Rows per page: 10

Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

Add metric data

Security analytics

Centralize security events for interactive investigation in ready-to-go visualizations.

Add security events

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

APM

Automatically collect in-depth performance metrics and errors from inside your applications.

Canvas

Showcase your data in a pixel-perfect way.

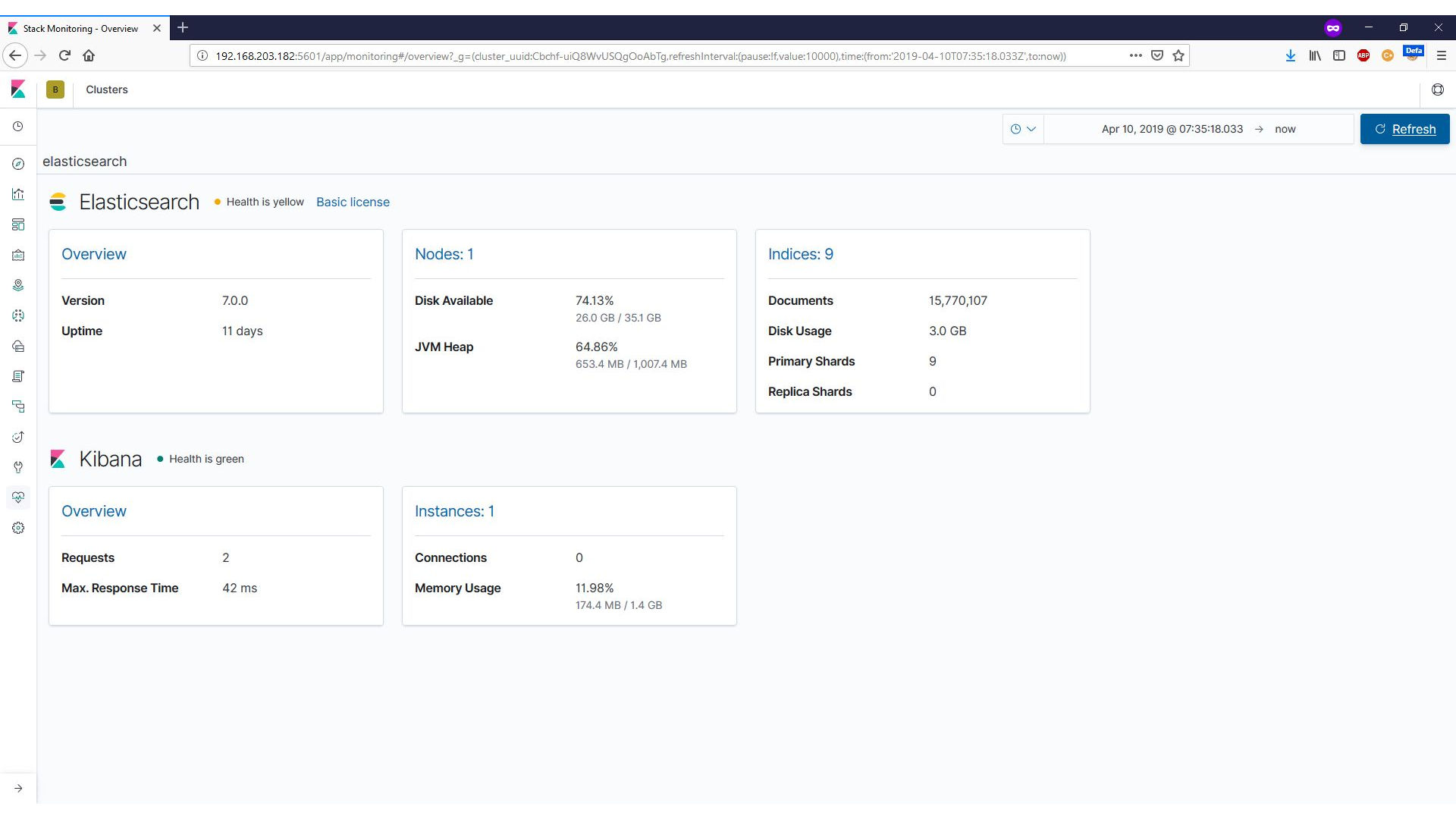
Manage and Administer the Elastic Stack

Console

Skip cURL and use this JSON interface to work with your data directly.

Index Patterns

Manage the index patterns that help retrieve your data from Elasticsearch.


Stack Monitoring - Overview
192.168.203.182:5601/app/monitoring#/overview?_g=(cluster_uuid:Cbchf-uiQ8WvUSQgOoAbTg,refreshInterval:(pause:!f,value:10000),time:(from:'2019-04-10T07:35:18.033Z',to:now))
Clusters
Apr 10, 2019 @ 07:35:18.033 → now
Refresh
elasticsearch
Elasticsearch
Health is yellow
Basic license
Overview
Version 7.0.0
Uptime 11 days
Nodes: 1
Disk Available 74.13%
26.0 GB / 35.1 GB
JVM Heap 64.86%
653.4 MB / 1,007.4 MB
Indices: 9
Documents 15,770,107
Disk Usage 3.0 GB
Primary Shards 9
Replica Shards 0
Kibana
Health is green
Overview
Requests 2
Max. Response Time 42 ms
Instances: 1
Connections 0
Memory Usage 11.98%
174.4 MB / 1.4 GB

Kibana

192.168.203.182:5601/app/uptime#/?_g=()

Overview

Uptime

Apr 10, 2019 @ 08:18:46.8 → Apr 23, 2019 @ 08:34:06.2

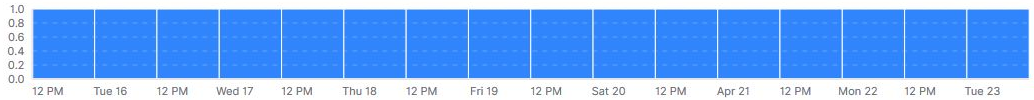
Search...

Up | Down | ID | Name | URL | Port | Scheme

Endpoint status

Up	Down	Total
1	0	1

Status over time



Monitor status

Status	Last updated	ID	URL	IP	Monitor History
Up	a few seconds ago	auto-http-0X5A13E1983C13A663	http://192.168.203.182:9200	192.168.203.182	

Rows per page: 10

Error list

Error type	Monitor ID	Count	Latest error	Status code	Latest message
No items found					

Rows per page: 10

[Filebeat System] Syslog dashb

192.168.203.182:5601/app/kibana#/dashboard/Filebeat-syslog-dashboard-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2019-04-10T08:22:35.813Z',to:now))&_a=(description:'Syslog

Dashboard / [Filebeat System] Syslog dashboard ECS

Full screen Share Clone Edit

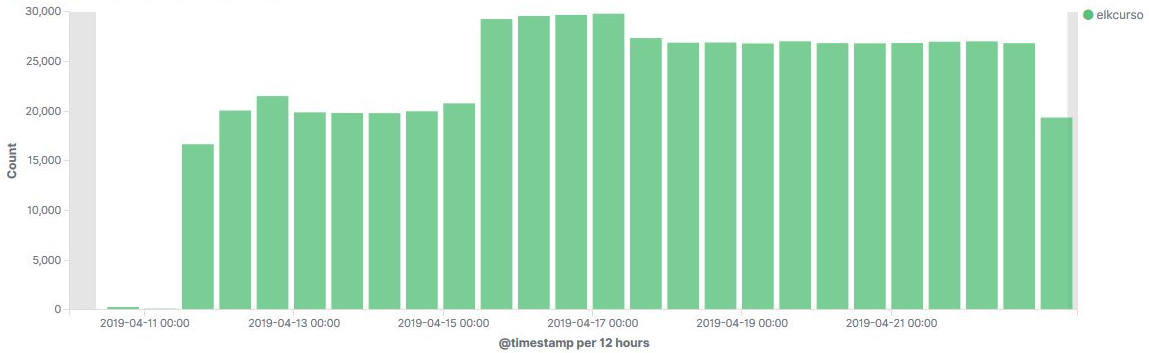
Filters * Lucene Apr 10, 2019 @ 08:22:35.813 → now Refresh

+ Add filter

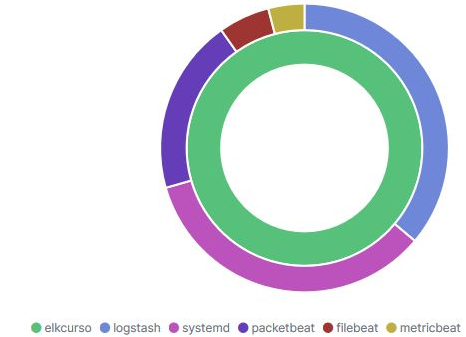
Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

Syslog events by hostname [Filebeat System] ECS



Syslog hostnames and processes [Filebeat System] ECS



Syslog logs [Filebeat System] ECS

1–50 of 593,508

Time	host.hostname	process.name	message
Apr 23, 2019 @ 08:36:31.000	elkcurso	systemd	logstash.service holdoff time over, scheduling restart.
Apr 23, 2019 @ 08:36:31.000	elkcurso	systemd	Stopped logstash.
Apr 23, 2019 @ 08:36:31.000	elkcurso	systemd	Started logstash.
Apr 23, 2019 @ 08:36:30.000	elkcurso	logstash	[2019-04-23T08:36:30,390][INFO][logstash.runner] Logstash shut down.
Apr 23, 2019 @ 08:36:30.000	elkcurso	systemd	logstash.service: main process exited, code=exited, status=1/FAILURE

Full screen Share Clone Edit

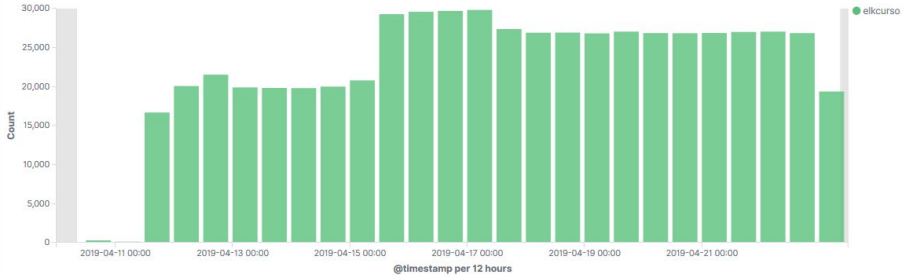
Filters * Lucene Apr 10, 2019 @ 08:22:35.813 → now Refresh

+ Add filter

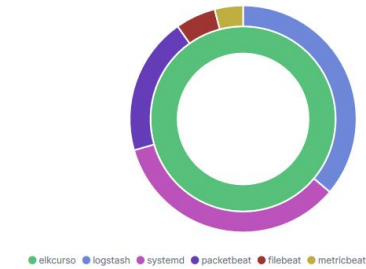
Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

Syslog events by hostname [Filebeat System] ECS



Syslog hostnames and processes [Filebeat System] ECS



Syslog logs [Filebeat System] ECS

1–50 of 593,508

Time	host.hostname	process.name	message
Apr 23, 2019 @ 08:36:31.000	elkcurso	systemd	logstash.service holdoff time over, scheduling restart.
Apr 23, 2019 @ 08:36:31.000	elkcurso	systemd	Stopped logstash.
Apr 23, 2019 @ 08:36:31.000	elkcurso	systemd	Started logstash.
Apr 23, 2019 @ 08:36:30.000	elkcurso	logstash	[2019-04-23T08:36:30,390][INFO][logstash.runner] Logstash shut down.
Apr 23, 2019 @ 08:36:30.000	elkcurso	systemd	logstash.service: main process exited, code=exited, status=1/FAILURE
Apr 23, 2019 @ 08:36:30.000	elkcurso	systemd	Unit logstash.service entered failed state.
Apr 23, 2019 @ 08:36:30.000	elkcurso	systemd	logstash.service failed.
Apr 23, 2019 @ 08:36:25.000	elkcurso	logstash	[2019-04-23T08:36:25,146][ERROR][logstash.javapipeline] Pipeline aborted due to error {:pipeline_id=>"main", :exception=>#<RegexpError: unmatched close parenthesis: /(?<SYSLOGTIMESTAMP:[system][auth][timestamp]>(?:\b(?:[Jj]an(?:uary|uar)?|[Ff]eb(?:ruary|ruar)?|[Mm](?:a|ÃÂª)r(?:ch|z)?|[Aa]pr(?:il)?|[Mm]a(?:y|j)?|[Jj]un(?:e|i)?|[Jj]ul(?:y)?|[Aa]ug(?:ust)?|[Ss]ep(?:tember)?|[Oo](?:c|k)?t(?:ober)?|[Nn]ov(?:ember)?|[Dd]e(?:c|z)(?:ember)?)\b) +(?:(?:0[1-9])|(?:[12][0-9])|(?:3[01]))|[1-9])) (?:(?!<[0-9])(?:(?:2[0123]|[01]?[0-9]):(?:(?:[0-5][0-9]))(?::(?:(?:[0-5]?[0-9]|60)(?:[:.,][0-9]+)?))?)|(?![0-9]))) (?<SYSLOGHOST:[system][auth][hostname]>(?:(?:(?:(?:(((?:[0-9A-Fa-f]{1,4}):){7}(?:[0-9A-Fa-f]{1,4}|:))|(((?:[0-9A-Fa-f]{1,4}):){6}(:|[0-9A-Fa-f]{1,4}|(?:(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}):))|(((?:[0-9A-Fa-f]{1,4}):){5}(((:[0-9A-Fa-f]{1,4})(1,2))|:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}):))|(((?:[0-9A-Fa-f]{1,4}):){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-f]{1,4})?:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))):)|(((?:[0-9A-Fa-f]{1,4}):){3}(((:[0-9A-Fa-f]{1,4}){1,4})|((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))):)|(((?:[0-9A-Fa-f]{1,4}):){2}(((:[0-9A-Fa-f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))):)|(((?:[0-9A-Fa-f]{1,4}):){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))):)|(:(((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)(\.(25[0-5]|2[0-4]\d|1\d\d|[1-9]?\d)){3}))):))(%.+?)|(?:(?<[0-9])(?:(?:0[1-9]|(?:[12][0-9])|(?:3[01]))|[1-9])) (?:(?!<[0-9])(?:(?:2[0123]|[01]?[0-9]):(?:(?:[0-5][0-9]))(?::(?:(?:[0-5]?[0-9]|60)(?:[:.,][0-9]+)?))?)|(?![0-9]))) (?<SYSLOGPROG:[system][auth][program]>(?:[^:]*)): +(?<SYSLOGMESSAGE:[system][auth][message]>(?:.*))$/ at [0]>
Apr 23, 2019 @ 08:36:25.000	elkcurso	logstash	[2019-04-23T08:36:25,172][ERROR][logstash.agent] Failed to execute action {:id=>:main, :action_type=>LogStash::ConvergeResult::FailedAction, :message=>"Could not execute action: PipelineAction::Create<main>, action_result: false", :backtrace=>nil}
Apr 23, 2019 @ 08:36:25.000	elkcurso	logstash	[2019-04-23T08:36:25,477][INFO][logstash.agent] Successfully started Logstash API endpoint {:port=>9600}
Apr 23, 2019 @ 08:36:24.000	elkcurso	logstash	[2019-04-23T08:36:24,594][INFO][logstash.filters.geoip] Using geoip database {:path=>"/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/logstash-filter-geoip-6.0.0-java/vendor/GeoLite2-City.mmdb"}
Apr 23, 2019 @ 08:36:21.000	elkcurso	packetbeat	2019-04-23T08:36:21.620+0200#011INFO#011[monitoring]#011log/log.go:144#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":29690,"time":{"ms":1}},"total":{"ticks":373220,"time":{"ms":4},"value":373220},"user":{"ticks":343530,"time":{"ms":3}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":6},"info":{"ephemeral_id":"3b2d0977-5008-4334-b53e-eb9efbdba972","uptime":{"ms":674280030}},"memstats":{"gc_next":74369296,"memory_alloc":38067816,"memory_total":6711549976}},"libbeat":{"config":{"module":{"running":0}},"pipeline":{"clients":15,"events":{"active":4117,"retry":50}}},"system":{"load":{"1":2.79,"15":2.59,"5":2.53,"norm":{"1":1.395,"15":1.295,"5":1.265}}}}}}

Full screen Share Clone Edit

Filters * Lucene Apr 10, 2019 @ 08:22:35.813 → now Update

+ Add filter

Dashboards [Filebeat System] ECS

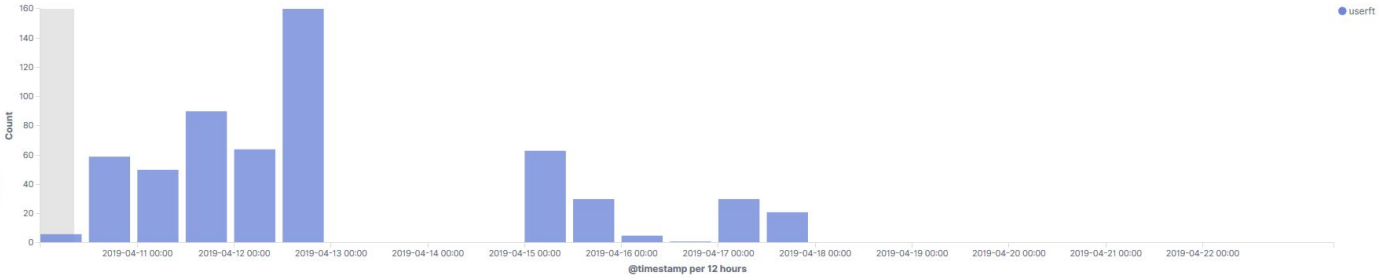
Syslog | Sudo commands | SSH logins | New users and groups

Top sudo commands [Filebeat System] ECS

/bin/nano filebeat.yml	userft	20
/sbin/service filebeat status	userft	20
/sbin/service filebeat restart	userft	17
/bin/yum install logstash	userft	14

Export: Raw Formatted

Sudo commands by user [Filebeat System] ECS



Sudo errors [Filebeat System] ECS

Full screen Share Clone Edit

Filters * Lucene Apr 10, 2019 @ 00:00:00.000 → now Update

+ Add filter

Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

Top sudo commands [Filebeat System] ECS

system.auth.sudo.command: Descending	user.name: Descending	Count
/sbin/service elasticsearch status	userft	46
/bin/nano filebeat.yml	userft	20
/sbin/service filebeat status	userft	20
/sbin/service filebeat restart	userft	17
/bin/yum install logstash	userft	14

Export: Raw Formatted

Sudo commands by user [Filebeat System] ECS

Sudo errors [Filebeat System] ECS

[Filebeat System] SSH login att

192.168.203.182:5601/app/kibana#/dashboard/5517a150-f9ce-11e6-8115-a7c18106d86a-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2019-04-10T08:22:35.813Z',to:now))&_a=

Dashboard / [Filebeat System] SSH login attempts ECS

Full screen Share Clone Edit

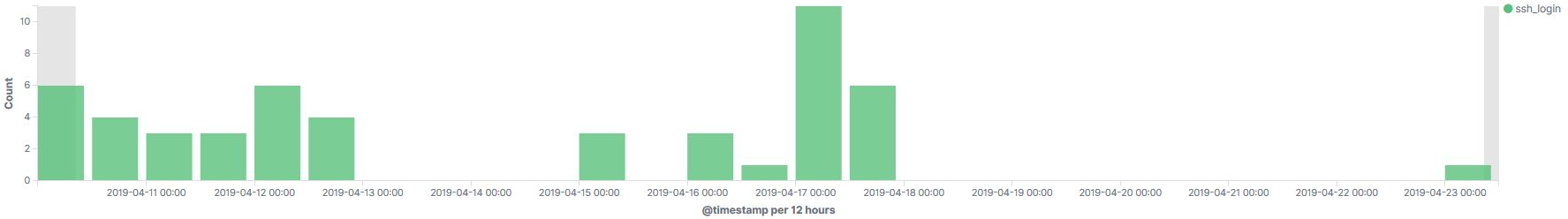
Filters * Lucene Apr 10, 2019 @ 08:22:35.813 → now Update

+ Add filter

Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

SSH login attempts [Filebeat System] ECS



Successful SSH logins [Filebeat System] ECS

No results found

SSH users of failed login attempts [Filebeat System] ECS

SSH failed login attempts source locations [Filebeat System] ECS

Full screen Share Clone Edit

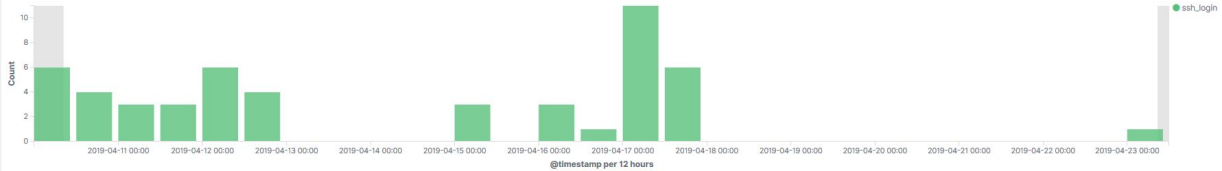
Filters * Lucene Apr 10, 2019 @ 08:22:35.813 → now Update

+ Add filter

Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

SSH login attempts [Filebeat System] ECS



Successful SSH logins [Filebeat System] ECS

No results found

SSH users of failed login attempts [Filebeat System] ECS

user.name: Descending - Count

SSH failed login attempts source locations [Filebeat System] ECS

SSH login attempts [Filebeat System] ECS

1–50 of 51

Time	event.action	system.auth.ssh.method	user.name	source.ip	source.geo.country_iso_code
Apr 23, 2019 @ 08:40:09.000	ssh_login	publickey	userft	192.168.203.133	-
Apr 17, 2019 @ 14:51:31.000	ssh_login	password	userft	10.212.134.3	-
Apr 17, 2019 @ 13:38:04.000	ssh_login	publickey	userft	192.168.203.133	-
Apr 17, 2019 @ 13:31:09.000	ssh_login	publickey	userft	192.168.203.133	-
Apr 17, 2019 @ 13:18:16.000	ssh_login	publickey	userft	192.168.203.133	-
Apr 17, 2019 @ 13:15:42.000	ssh_login	publickey	userft	192.168.203.133	-

[Filebeat System] New users an

192.168.203.182:5601/app/kibana#/dashboard/0d3f2380-fa78-11e6-ae9b-81e5311e8cab-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2019-04-10T08:22:35.813Z',to:now))&_a=

Dashboard / [Filebeat System] New users and groups ECS

Full screen Share Clone Edit

Filters * Lucene Apr 10, 2019 @ 08:22:35.813 → now Update

Click to apply

+ Add filter

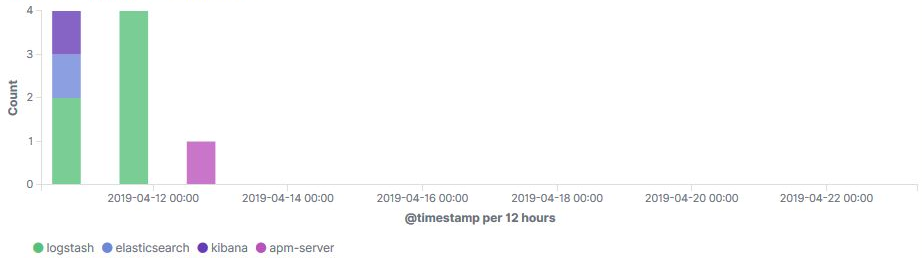
Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

New users [Filebeat System] ECS

Host	User	UID	GID	Home	Shell	Count
elkcurso	logstash	995	993	/usr/share/logstash	/sbin/nologin	5
elkcurso	logstash	997	995	/usr/share/logstash	/sbin/nologin	1
elkcurso	apm-server	994	992	/var/lib/apm-server	/bin/bash	1
elkcurso	elasticsearch	998	996	/nonexistent	/sbin/nologin	1
elkcurso	kibana	996	994	/home/kibana	/sbin/nologin	1

New users over time [Filebeat System] ECS



New users by shell [Filebeat System] ECS

New users by home directory [Filebeat System] ECS

New groups [Filebeat System] ECS

New groups over time [Filebeat System] ECS

Discover - Kibana

192.168.203.182:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2019-04-10T08:22:35.813Z',to:now))&_a=(columns:!(_source),index:'filebeat-*',interval:auto,q

Discover

7,888,555 hits

New Save Open Share Inspect

Filters Search KQL Apr 10, 2019 @ 08:22:35.813 → now Refresh

+ Add filter

filebeat-*

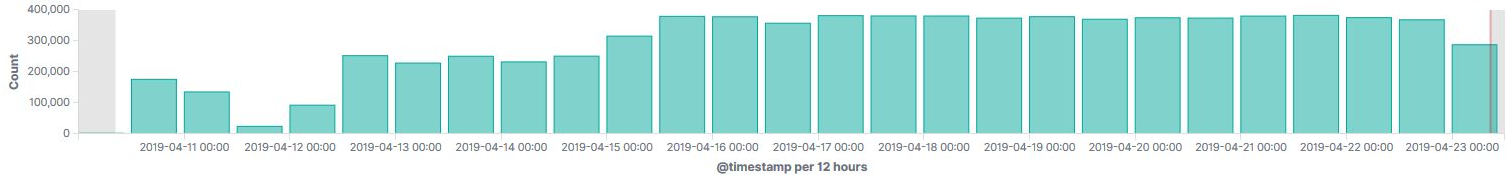
Selected fields

? _source

Available fields

@timestamp
t _id
t _index
_score
t _type
t agent.ephemeral_id
t agent.hostname
t agent.id
t agent.type
t agent.version
t ecs.version
t elasticsearch.gc.tags
elasticsearch.gc.young_gen.size_kb
elasticsearch.gc.young_gen.used_kb
event.created
t event.dataset
t event.module
t fileset.name

Apr 10, 2019 @ 08:22:35.813 - Apr 23, 2019 @ 08:42:20.759 — Auto



Time	_source
Apr 23, 2019 @ 08:42:18.000	agent.hostname: elkcurso.localdomain agent.id: 61d8dddf-9437-4d0c-a067-7325950f8ef7 agent.type: filebeat agent.ephemeral_id: 68423f62-0b9d-4351-a782-7878a02a5f57 agent.version: 7.0.0 process.name: metricbeat log.file.path: /var/log/messages log.offset: 57,376,360 fileset.name: syslog message: 2019-04-23T08:42:18.679+0200#011INFO#011[monitoring]#011log/log.go:144#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":3155090,"time":{"ms":132}},"total":{"ticks":6201020,"time":{"ms":269},"value":6201020},"user":{"ticks":3045930,"time":{"ms":137}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":6},"info":{"ephemeral_id":"47e0e2ac-9786-46fd-bb37-e2a8d87b5ceb","uptime":{"ms":689970056}},"memstats":{"gc_next":11869872,"memory_alloc":7606768,"memory_total":777528708640}},"libbeat":{"config":{"module":{"running":0}},"output":{"ev
Apr 23, 2019 @ 08:42:17.000	agent.hostname: elkcurso.localdomain agent.id: 61d8dddf-9437-4d0c-a067-7325950f8ef7 agent.type: filebeat agent.ephemeral_id: 68423f62-0b9d-4351-a782-7878a02a5f57 agent.version: 7.0.0 process.name: heartbeat log.file.path: /var/log/messages log.offset: 57,375,481 fileset.name: syslog message: 2019-04-23T08:42:17.132+0200#011INFO#011[monitoring]#011log/log.go:144#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":73110,"time":{"ms":5}},"total":{"ticks":180470,"time":{"ms":8},"value":180470},"user":{"ticks":107360,"time":{"ms":3}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":7},"info":{"ephemeral_id":"9c4a6972-4d44-4f47-b8af-5f3827fca1d5","uptime":{"ms":689400021}},"memstats":{"gc_next":4194304,"memory_alloc":3275544,"memory_total":24312751696}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked"
Apr 23, 2019 @ 08:42:12.000	agent.hostname: elkcurso.localdomain agent.id: 61d8dddf-9437-4d0c-a067-7325950f8ef7 agent.type: filebeat agent.ephemeral_id: 68423f62-0b9d-4351-a782-7878a02a5f57 agent.version: 7.0.0 process.name: filebeat log.file.path: /var/log/messages log.offset: 57,374,392 fileset.name: syslog message: 2019-04-23T08:42:12.022+0200#011INFO#011[monitoring]#011log/log.go:144#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":1126610,"time":{"ms":45}},"total":{"ticks":3463290,"time":{"ms":118},"value":3463290},"user":{"ticks":2336680,"time":{"ms":73}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":14},"info":{"ephemeral_id":"68423f62-0b9d-4351-a782-7878a02a5f57","uptime":{"ms":930180034}},"memstats":{"gc_next":7437568,"memory_alloc":5509848,"memory_total":428833582008}},"filebeat":{"events":{"added":489,"done":489},"harvester":{"op
Apr 23, 2019 @ 08:42:05.000	agent.hostname: elkcurso.localdomain agent.id: 61d8dddf-9437-4d0c-a067-7325950f8ef7 agent.type: filebeat agent.ephemeral_id: 68423f62-0b9d-4351-a782-7878a02a5f57 agent.version: 7.0.0 process.name: sudo log.file.path: /var/log/secure log.offset: 1,328 fileset.name: auth message: pam_unix(sudo:session): session closed for user root input.type: log @timestamp: Apr 23, 2019 @ 08:42:05.000 ecs.version: 1.0.0 service.type: system host.hostname: elkcurso host.os.kernel: 3.10.0-957.el7.x86_64 host.os.codename: Core host.os

Discover - Kibana

192.168.203.182:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2019-04-10T08:22:35.813Z',to:now))&_a=(columns:!(_source),index:'metricbeat-*',interval:aut

Discover

964,688 hits

New Save Open Share Inspect

Filters Search KQL Apr 10, 2019 @ 08:22:35.813 → now Refresh

+ Add filter

metricbeat-*

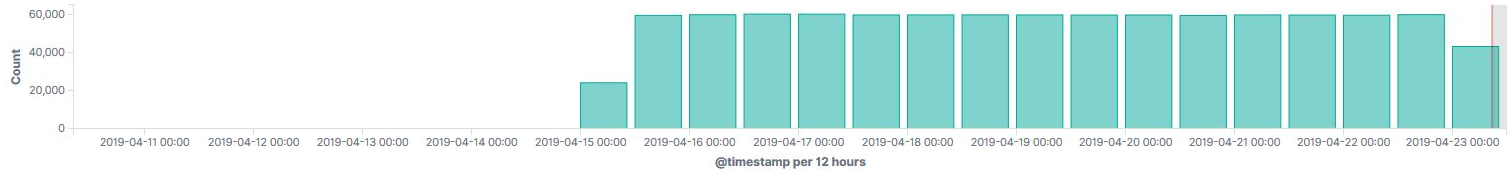
Selected fields

? _source

Available fields

@timestamp
t _id
t _index
_score
t _type
t agent.ephemeral_id
t agent.hostname
t agent.id
t agent.type
t agent.version
t ecs.version
t event.dataset
event.duration
t event.module
t host.architecture
host.containerized
t host.hostname
t host.id

Apr 10, 2019 @ 08:22:35.813 - Apr 23, 2019 @ 08:42:54.203 — Auto



Time	_source
Apr 23, 2019 @ 08:42:31.685	@timestamp: Apr 23, 2019 @ 08:42:31.685 metricset.name: network event.dataset: system.network event.module: system event.duration: a few seconds service.type: system system.network.in.bytes: 30.647GB system.network.in.packets: 28,280,687 system.network.in.errors: 0 system.network.in.dropped: 0 system.network.out.errors: 0 system.network.out.dropped: 0 system.network.out.packets: 28,280,687 system.network.out.bytes: 30.647GB system.network.name: lo ecs.version: 1.0.0 host.containerized: true host.name: elkcurso.localdomain host.hostname: elkcurso.localdomain host.architecture: x86_64 host.os.kernel: 3.10.0-957.el7.x86_64 host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.os.family: redhat host.os.name: CentOS Linux host.id: 066e544b1e644b5da156d598ed2d4ed2 agent.version: 7.0.0 agent.type: metricbeat agent.ephemeral_id: 47e0e2ac-
Apr 23, 2019 @ 08:42:31.685	@timestamp: Apr 23, 2019 @ 08:42:31.685 service.type: system system.network.in.bytes: 2.953GB system.network.in.packets: 4,747,962 system.network.in.errors: 0 system.network.in.dropped: 2,640 system.network.out.errors: 0 system.network.out.dropped: 0 system.network.out.packets: 1,352,344 system.network.out.bytes: 206.711MB system.network.name: ens160 ecs.version: 1.0.0 host.containerized: true host.hostname: elkcurso.localdomain host.architecture: x86_64 host.name: elkcurso.localdomain host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.os.family: redhat host.os.name: CentOS Linux host.os.kernel: 3.10.0-957.el7.x86_64 host.id: 066e544b1e644b5da156d598ed2d4ed2 agent.type: metricbeat agent.ephemeral_id: 47e0e2ac-9786-46fd-bb37-e2a8d87b5ceb agent.hostname: elkcurso.localdomain agent.id: 4f32468c-c447-4d85-ac27-68d6b85dd328 agent.ve
Apr 23, 2019 @ 08:42:31.685	@timestamp: Apr 23, 2019 @ 08:42:31.685 service.type: system system.process.summary.idle: 0 system.process.summary.stopped: 0 system.process.summary.zombie: 0 system.process.summary.unknown: 0 system.process.summary.dead: 0 system.process.summary.total: 117 system.process.summary.sleeping: 116 system.process.summary.running: 1 agent.ephemeral_id: 47e0e2ac-9786-46fd-bb37-e2a8d87b5ceb agent.hostname: elkcurso.localdomain agent.id: 4f32468c-c447-4d85-ac27-68d6b85dd328 agent.version: 7.0.0 agent.type: metricbeat ecs.version: 1.0.0 host.os.name: CentOS Linux host.os.kernel: 3.10.0-957.el7.x86_64 host.os.codename: Core host.os.platform: centos host.os.version: 7 (Core) host.os.family: redhat host.id: 066e544b1e644b5da156d598ed2d4ed2 host.containerized: true host.name: elkcurso.localdomain host.hostname: elkcurso.localdomain host.architecture: x86_64 event.datase
Apr 23, 2019 @ 08:42:31.685	@timestamp: Apr 23, 2019 @ 08:42:31.685 system.socket.summary.all.count: 80 system.socket.summary.all.listening: 8 system.socket.summary.tcp.all.time_wait: 8 system.socket.summary.tcp.all.count: 80 system.socket.summary.tcp.all.listening: 8 system.socket.summary.tcp.all.established: 63 system.socket.summary.tcp.all.close_wait: 1 system.socket.summary.udp.all.count: 0 ecs.version: 1.0.0 host.name: elkcurso.localdomain host.architecture: x86_64 host.os.family: redhat host.os.name: CentOS Linux host.os.kernel: 3.10.0-9

Discover - Kibana

192.168.203.182:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2019-04-10T08:22:35.813Z',to:now))&_a=(columns:!(_source),index:'apm-*',interval:auto,quer

Discover

2 hits

New Save Open Share Inspect

Filters Search KQL Apr 10, 2019 @ 08:22:35.813 → now Refresh

+ Add filter

apm-*

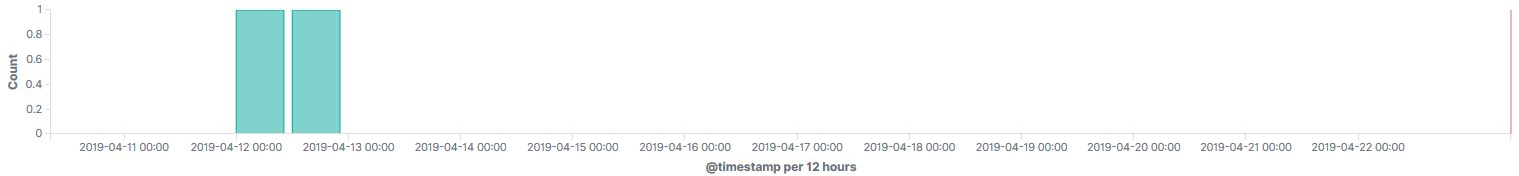
Selected fields

? _source

Available fields

@timestamp
t _id
t _index
_score
t _type
t ecs.version
? observer.ephemeral_id
t observer.hostname
? observer.id
t observer.listening
t observer.type
t observer.version
observer.version_major
t processor.event
t processor.name

Apr 10, 2019 @ 08:22:35.813 - Apr 23, 2019 @ 08:43:27.404 — Auto

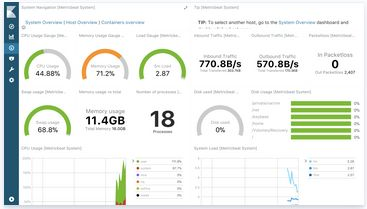


Time	_source
Apr 12, 2019 @ 12:07:13.169	observer.listening: 192.168.203.182:8200 observer.hostname: elkcurso.localdomain observer.id: ce9aaa2d-ca39-448b-bce2-6dd6f554307b observer.ephemeral_id: 40ae019a-2a34-4861-92a0-5009143950c6 observer.type: apm-server observer.version: 7.0.0 observer.version_major: 7 @timestamp: Apr 12, 2019 @ 12:07:13.169 ecs.version: 1.1.0-dev processor.name: onboarding processor.event: onboarding _id: Gp1xEWoBZ_nWQmF-1j42 _type: _doc _index: apm-7.0.0-onboarding-2019.04.12 _score: -
Apr 12, 2019 @ 11:57:49.709	observer.listening: 192.168.203.182:8200 observer.hostname: elkcurso.localdomain observer.id: ce9aaa2d-ca39-448b-bce2-6dd6f554307b observer.ephemeral_id: ebd4c29f-6ae2-43b4-b9f5-af0afb78654b observer.type: apm-server observer.version: 7.0.0 observer.version_major: 7 @timestamp: Apr 12, 2019 @ 11:57:49.709 ecs.version: 1.1.0-dev processor.name: onboarding processor.event: onboarding _id: 2Z1pEWoBZ_nWQmF-PiJF _type: _doc _index: apm-7.0.0-onboarding-2019.04.12 _score: -

System metrics

The `system` Metricbeat module collects CPU, memory, network, and disk statistics from the host. It collects system wide statistics and statistics per process and filesystem. Learn more.

View exported fields



Self managed | Elastic Cloud

Getting Started

macOS | DEB | RPM | Windows

1 Download and install Metricbeat

First time using Metricbeat? See the Getting Started Guide.

Copy snippet

```
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.0.0-x86_64.rpm
sudo rpm -vi metricbeat-7.0.0-x86_64.rpm
```

Looking for the 32-bit packages? See the Download page.

2 Edit the configuration

Modify `/etc/metricbeat/metricbeat.yml` to set the connection information:

Copy snippet

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
```

System metrics

The `system` Metricbeat module collects CPU, memory, network, and disk statistics from the host. It collects system wide statistics and statistics per process and filesystem. Learn more.

View exported fields

Self managed | Elastic Cloud

Getting Started

macOS | DEB | RPM | Windows

1 Download and install Metricbeat

First time using Metricbeat? See the Getting Started Guide.

Copy snippet

```
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.0.0-x86_64.rpm
sudo rpm -vi metricbeat-7.0.0-x86_64.rpm
```

Looking for the 32-bit packages? See the Download page.

2 Edit the configuration

Modify `/etc/metricbeat/metricbeat.yml` to set the connection information:

Copy snippet

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
setup.kibana:
  host: "<kibana_url>"
```

Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

3 Enable and configure the system module

Copy snippet

```
sudo metricbeat modules enable system
```

Modify the settings in the `/etc/metricbeat/modules.d/system.yml` file.

4 Start Metricbeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

Copy snippet

```
sudo metricbeat setup
sudo service metricbeat start
```

Module status

Check that data is received from the Metricbeat `system` module

Check data

When all steps are complete, you're ready to explore your data.

System metrics dashboard

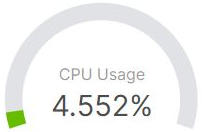
System Navigation [Metricbeat System] ECS

System Overview | Host Overview | Containers overview

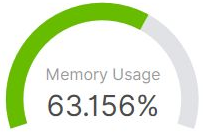
Number of hosts [Metricbeat System] ECS

1

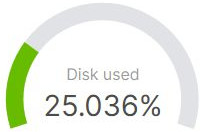
CPU Usage Gauge [Metricbeat System] ECS



Memory Usage Gauge [Metricbeat System] ...



Disk used [Metricbeat System] ECS



Inbound Traffic [Metricbeat System] ECS

Inbound Traffic
273.952B/s
Total Transferred 280.833MB

Outbound Traffic [Metricbeat System] ECS

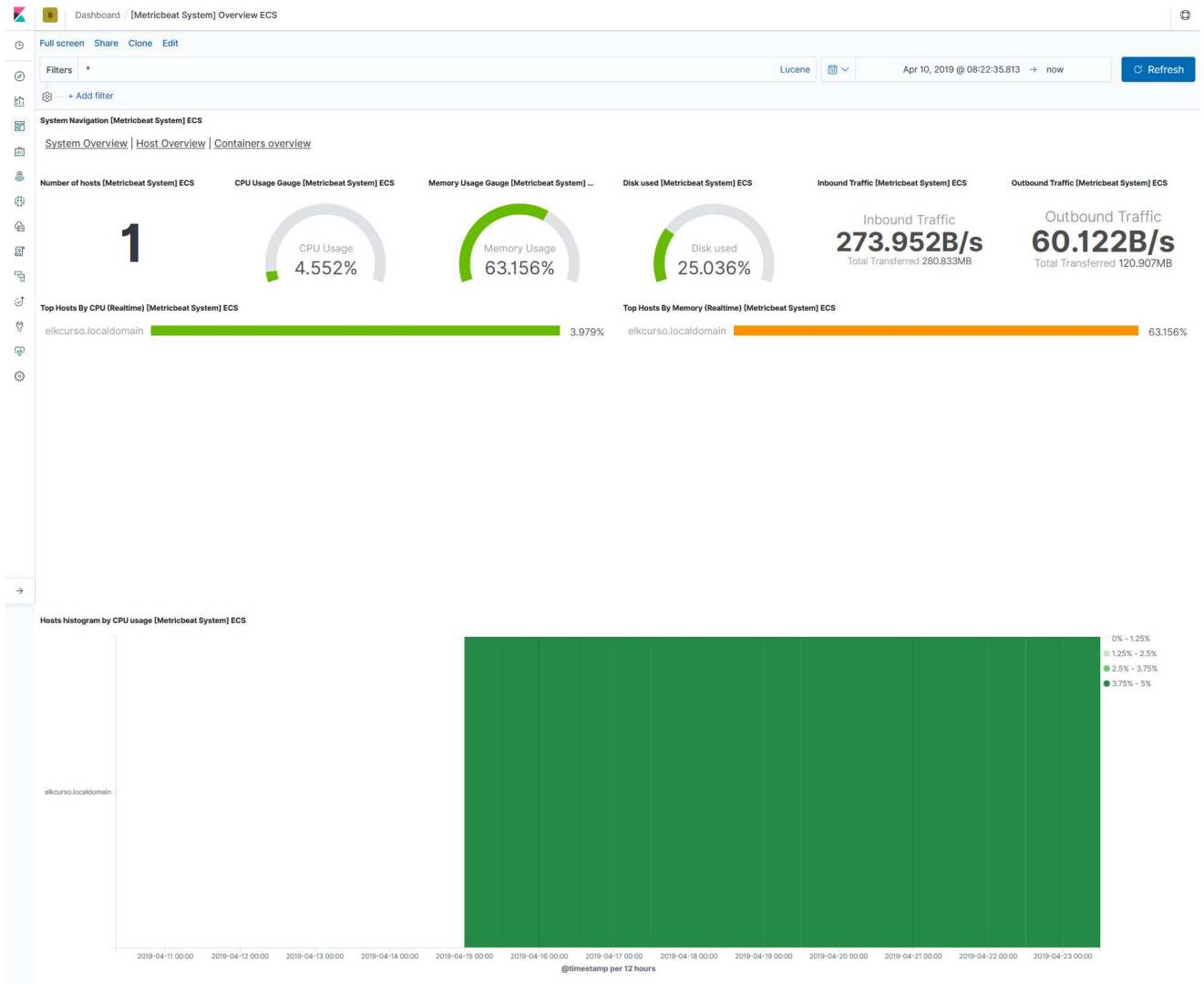
Outbound Traffic
60.122B/s
Total Transferred 120.907MB

Top Hosts By CPU (Realtime) [Metricbeat System] ECS

elkcurso.localdomain 3.979%

Top Hosts By Memory (Realtime) [Metricbeat System] ECS

elkcurso.localdomain 63.156%


Dashboard / [Metricbeat System] Overview ECS
Full screen Share Clone Edit
Filters *
Lucene
Apr 10, 2019 @ 08:22:35.813 → now
Refresh
+ Add filter
System Navigation [Metricbeat System] ECS
System Overview | Host Overview | Containers overview
Number of hosts [Metricbeat System] ECS
1
CPU Usage Gauge [Metricbeat System] ECS
CPU Usage
4.552%
Memory Usage Gauge [Metricbeat System] ...
Memory Usage
63.156%
Disk used [Metricbeat System] ECS
Disk used
25.036%
Inbound Traffic [Metricbeat System] ECS
Inbound Traffic
273.952B/s
Total Transferred 280.833MB
Outbound Traffic [Metricbeat System] ECS
Outbound Traffic
60.122B/s
Total Transferred 120.907MB
Top Hosts By CPU (Realtime) [Metricbeat System] ECS
elkcurso.localdomain
3.979%
Top Hosts By Memory (Realtime) [Metricbeat System] ECS
elkcurso.localdomain
63.156%
Hosts histogram by CPU usage [Metricbeat System] ECS
elkcurso.localdomain
0% - 1.25%
1.25% - 2.5%
2.5% - 3.75%
3.75% - 5%
2019-04-11 00:00
2019-04-12 00:00
2019-04-13 00:00
2019-04-14 00:00
2019-04-15 00:00
2019-04-16 00:00
2019-04-17 00:00
2019-04-18 00:00
2019-04-19 00:00
2019-04-20 00:00
2019-04-21 00:00
2019-04-22 00:00
2019-04-23 00:00
@timestamp per 12 hours

[Metricbeat System] Host overv

192.168.203.182:5601/app/kibana#/dashboard/79ffd6e0-faa0-11e6-947f-177f697178b8-ecs?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2019-04-10T08:22:35.813Z',to:now))&_a=(

Dashboard / [Metricbeat System] Host overview ECS

Full screen Share Clone Edit

Filters host.name:"elkcurso.localdomain" Lucene Apr 10, 2019 @ 08:22:35.813 → now Refresh

+ Add filter

System Navigation [Metricbeat System] ECS

System Overview | Host Overview | Containers overview

Tip [Metricbeat System] ECS

TIP: To select another host, go to the System Overview dashboard and double-click a host name.

CPU Usage Gauge [Metricbeat System] ECS

CPU Usage
4.552%

Memory Usage Gauge [Metricbeat System] ...

Memory Usage
63.156%

Load Gauge [Metricbeat System] ECS

5m Load
2.499

Inbound Traffic [Metricbeat System] ECS

Inbound Traffic
273.952B/s
Total Transferred 280.875MB

Outbound Traffic [Metricbeat System] ECS

Outbound Traffic
60.122B/s
Total Transferred 120.926MB

Packetloss [Metricbeat System] ECS

In Packetloss
2,640
Out Packetloss 0

Swap usage [Metricbeat System] ECS

Swap usage
8.144%

Memory usage vs total ECS

Memory usage
2.437GB
Total Memory 3.858GB

Number of processes [Metricbeat System] E...

15,777
Processes

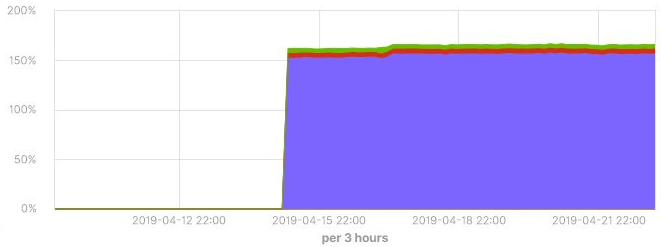
Disk used [Metricbeat System] ECS

Disk used
25.036%

Disk Usage [Metricbeat System] ECS

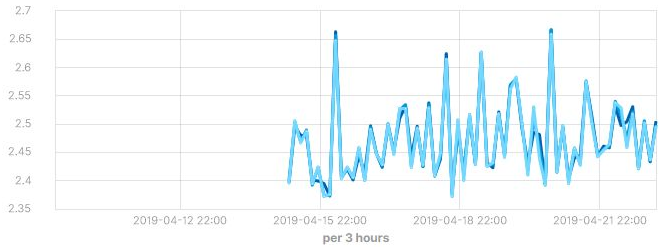
/ 25.294%

CPU Usage [Metricbeat System] ECS

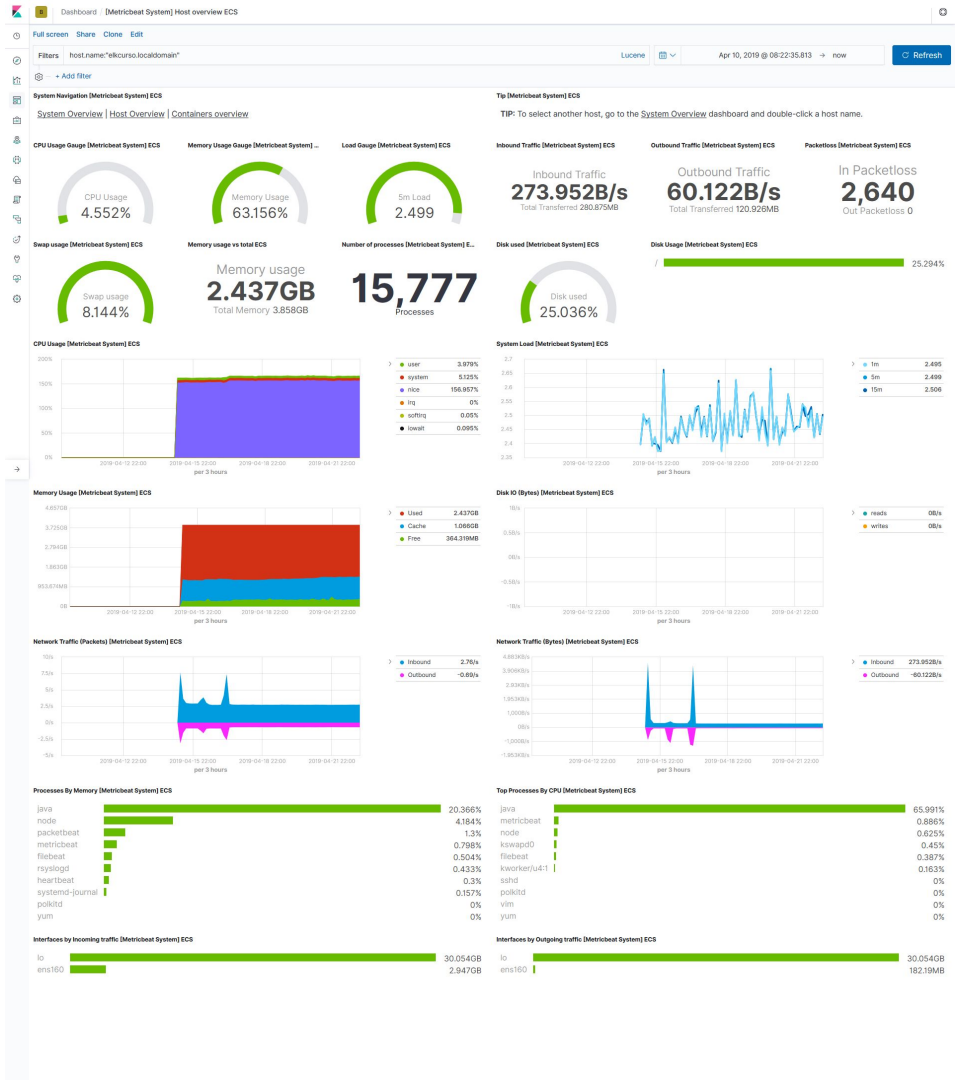


user	3.979%
system	5.125%
nice	156.957%
irq	0%
softirq	0.05%
iowait	0.095%

System Load [Metricbeat System] ECS



1m	2.495
5m	2.499
15m	2.506


Dashboard / [Metricbeat System] Host overview ECS
Full screen Share Clone Edit
Filters host.name:"elkcurso.localdomain" Lucene Apr 10, 2019 @ 08:22:35.813 → now Refresh
+ Add filter
System Navigation [Metricbeat System] ECS
System Overview | Host Overview | Containers overview
Tip [Metricbeat System] ECS
TIP: To select another host, go to the System Overview dashboard and double-click a host name.
CPU Usage Gauge [Metricbeat System] ECS
CPU Usage 4.552%
Memory Usage Gauge [Metricbeat System] ...
Memory Usage 63.156%
Load Gauge [Metricbeat System] ECS
5m Load 2.499
Inbound Traffic [Metricbeat System] ECS
Inbound Traffic 273.952B/s
Total Transferred 280.879MB
Outbound Traffic [Metricbeat System] ECS
Outbound Traffic 60.122B/s
Total Transferred 120.926MB
Packetloss [Metricbeat System] ECS
In Packetloss 2,640
Out Packetloss 0
Swap usage [Metricbeat System] ECS
Swap usage 8.144%
Memory usage vs total ECS
Memory usage 2.437GB
Total Memory 3.858GB
Number of processes [Metricbeat System] E...
15,777
Processes
Disk used [Metricbeat System] ECS
Disk used 25.036%
Disk Usage [Metricbeat System] ECS
/ 25.294%
CPU Usage [Metricbeat System] ECS
user 3.979%
system 5.125%
nice 156.957%
irq 0%
softirq 0.05%
iowait 0.095%
per 3 hours
System Load [Metricbeat System] ECS
1m 2.495
5m 2.499
15m 2.506
per 3 hours
Memory Usage [Metricbeat System] ECS
Used 2.437GB
Cache 1.069GB
Free 364.319MB
per 3 hours
Disk IO (Bytes) [Metricbeat System] ECS
reads 0B/s
writes 0B/s
per 3 hours
Network Traffic (Packets) [Metricbeat System] ECS
Inbound 2.76/s
Outbound -0.69/s
per 3 hours
Network Traffic (Bytes) [Metricbeat System] ECS
Inbound 273.952B/s
Outbound -60.122B/s
per 3 hours
Processes By Memory [Metricbeat System] ECS
java 20.366%
node 4.184%
packetbeat 1.3%
metricbeat 0.798%
filebeat 0.504%
rsyslogd 0.433%
heartbeat 0.3%
systemd-journal 0.157%
polkitd 0%
yum 0%
Top Processes By CPU [Metricbeat System] ECS
java 65.991%
metricbeat 0.886%
node 0.625%
kswapd0 0.45%
filebeat 0.387%
kworker/u4:1 0.163%
sshd 0%
polkitd 0%
vim 0%
yum 0%
Interfaces by Incoming traffic [Metricbeat System] ECS
lo 30.054GB
ens160 2.947GB
Interfaces by Outgoing traffic [Metricbeat System] ECS
lo 30.054GB
ens160 182.19MB

ES VITORIA CIBERSEGURIDAD ED 1

INFORMACIÓN RELEVANTE PARA EL CURSO

Si quieres ver más vídeos accede a **#ConectaEmpleo**

En esta primera sección podrás encontrar información relevante del curso como:

- La carta de compromiso
- El calendario del curso
- Políticas de justificantes y ausencias
- Los eventos relacionados con el curso más destacados

© Desarrollado por Telefónica Educación Digital

2019 abril

LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES	SÁBADO	DOMINGO
01	02	03	04	05	06	07
M9. Metasploit	M10. Vulneración de mecanismos de identificación y autentización	M10. Vulneración de mecanismos de identificación y autentización	M11.PROYECTO FINAL	M11.PROYECTO FINAL		
08	09	10	11	12	13	14
M11.PROYECTO FINAL	M11.PROYECTO FINAL	M11.PROYECTO FINAL	M11.PROYECTO FINAL	M11.PROYECTO FINAL		
15	16	17	18	19	20	21
M11.PROYECTO FINAL	M11.PROYECTO FINAL	M11.PROYECTO FINAL	VACACIONES	VACACIONES		
22	23	24	25	26	27	28
VACACIONES	M11.PROYECTO FINAL	M11.PROYECTO FINAL	Habilidades de Empleo y Emprendimiento	Habilidades de Empleo y Emprendimiento		
29	30	01	02	03	04	05
VACACIONES	VACACIONES					
06	07					

- Reunión BeClever
- Laboratorio
- Servidor en producción
- Configuraciones
- Entrega final

2019 mayo

LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES	SÁBADO	DOMINGO
29	30	01	02	03	04	05
		VACACIONES	M11.PROYECTO FINAL	M11.PROYECTO FINAL		
06	07	08	09	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	01	02
03	04					

- Reunión BeClever
- Laboratorio
- Servidor en producción
- Configuraciones
- Entrega final

El Cyber Range del nodo de ciberseguridad del BDIH, una infraestructura puntera para la capacitación de profesionales

01/04/2019 | | PDF DOCX | RSS

El Gobierno Vasco puso en marcha el año pasado el nodo de ciberseguridad del Basque Digital Innovation Hub con el objetivo de promover el desarrollo de proyectos de I+D+I.

El nodo de ciberseguridad, puntero en su sector, está formado por 5 laboratorios distribuidos por todo Euskadi.

Conecta Empleo es un proyecto social de Fundación Telefónica para formar en habilidades digitales a personas para mejorar su inserción laboral en base a las tecnologías y competencias con más demanda laboral (Big data, desarrollo web y de aplicaciones móviles, programación de videojuegos, y ciberseguridad).

El pasado 28 de marzo, un grupo de alumnos pertenecientes a la formación en ciberseguridad que se está impartiendo en la actualidad en Vitoria-Gasteiz asistió al Cyber Range del nodo de ciberseguridad del **Basque Digital Innovation Hub** para realizar un ejercicio de entrenamiento.

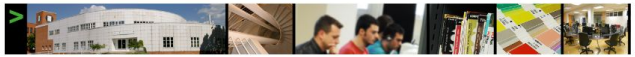
El Cyber Range es una plataforma que permite simular entornos reales para la formación y el entrenamiento individual o colectivo de profesionales. Estos entornos permiten realizar ejercicios de securización de sistemas, poner en práctica técnicas y tácticas tanto de ataque como de defensa, etc. Para ello, se llevan a cabo escenarios de **Read Team vs Blue Team**, en el que un grupo de participantes ataca una infraestructura mientras otro la defiende, o **Capture The Flag (CTF)**, en el que hay que resolver una serie de pruebas.

En esta ocasión, los alumnos de la Fundación Telefónica participaron en un escenario de CTF en el que realizaron ejercicios de entrenamiento diseñados para identificar las vulnerabilidades más habituales en aplicaciones web, y aprendieron a implementar controles para protegerlas.

Nodo de ciberseguridad

El Gobierno Vasco, a través del Basque Cybersecurity Centre, *SPRI* y los agentes de la Red Vasca de Ciencia Tecnología e Innovación (Tecnalia, Ikerlan, Vicomtech y BCAM), puso en marcha el año pasado el **nodo de ciberseguridad del Basque Digital Innovation Hub**. En la actualidad, en el BDIH hay 3 nodos activos: Fabricación aditiva; Robótica flexible; y Ciberseguridad.

CETIC (Centro de Tecnologías de la Información y Comunicación)



CETIC (Centro de Tecnologías de la Información y la Comunicación) ofrece un conjunto de recursos y actividades orientados a fomentar la capacitación profesional, el reciclaje y la inserción laboral a través de la realización de acciones de formación, orientación e información y el contacto con las empresas dentro del sector TIC.

Contacto

- C/ Castro Urdiales, 10
- Tfno: 945 16 15 05 / Fax: 945 16 15 04
- formacionempleo@vitoria-gasteiz.org

Horarios

- Centro:
  - Horario normal: de lunes a viernes, de 8:00 a 21:00.
  - Del 6 al 17 de agosto: cerrado.
  - Del 20 al 24 de agosto: abierto de 8:00 a 14:00.
- Centro de Empleo:
  - Horario normal: de lunes a viernes, de 9:00 a 20:00.
  - Del 30 de julio al 31 de agosto: cerrado.
  - Del 3 al 14 de septiembre: abierto de 8:00 a 14:00.
  - Navidad: cerrado hasta el 6 de enero.
- Servicio de elearning:
  - Horario normal: de lunes a viernes, de 9:00 a 21:00.
  - Del 2 al 27 de julio: de 8.00 a 14.00.
  - Del 30 de julio al 14 de septiembre: cerrado.
  - Navidad: cerrado hasta el 6 de enero.

Recursos

- Biblioteca
- Alquiler de instalaciones (Ordenanza 8.8: Precio Público para la Prestación de Servicios de Formación Profesional Ocupacional y Continua del Departamento de Promoción Económica)

Destacamos

Taller de activación laboral (abril)

Nueva oferta formativa

Martes tecnológicos

Búsqueda de empleo

- Orientación e intermediación laboral
- Centro de empleo
- Orientación formativa
- Taller de activación laboral
- Coaching para la búsqueda de empleo
- Talleres específicos y breves
- Empleo joven
- Guía GPS - Orientación académico-profesional para jóvenes
- Otros recursos

Formación para el empleo

- Programas presenciales
- Programas e-learning
- Jornadas construcción sostenible
- Consulta e inscripción en programas

Centros

- CETIC
- Centro Ignacio Ellacuría

Más información


TO START
PRESS ANY KEY
"To start, press any key."
Where's the "any" key?

OSSEC... Open Source HIDS Security.

OSSEC http://www.ossec.net/, sistema Open Source de detección de intrusiones basado en host (HIDS) y ELK (Elasticsearch, Logstash, and Kibana) como un sistema unificado de información de seguridad y gestión de eventos (SIEM). Se emplea para detectar intrusiones, uso indebido de software, rootkits o configuraciones de seguridad débiles, entre otras cosas.

- https://github.com/ossec/ossec-hids
- http://www.ossec.net/blog.html
- http://www.ossec.net/docs/
- http://www.ossec.net/downloads.html
- https://atomicorp.com/atomic-secured-ossec/

Watching

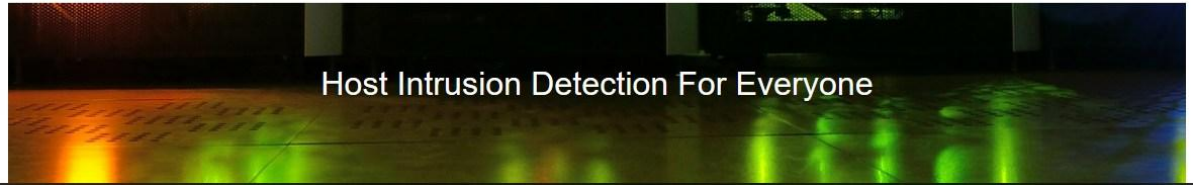
OSSEC watches it all, actively monitoring all aspects of system activity with file integrity monitoring, log monitoring, rootcheck, and process monitoring. With OSSEC you won't be in the dark about what is happening to your valuable computer system assets.

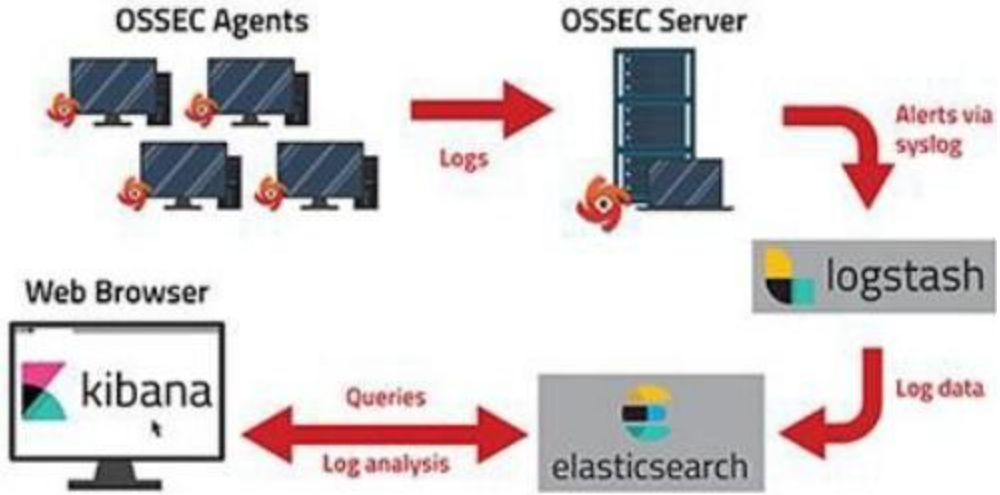
Alerting

When attacks happen OSSEC lets you know through alert logs and email alerts sent to you and your IT staff so you can take quick actions. OSSEC also exports alerts to any SIEM system via syslog so you can get real-time analytics and insights into your system security events.

Everywhere

Got a variety of operating systems to support and protect? OSSEC has you covered with comprehensive host based intrusion detection across multiple platforms including Linux,Solaris, AIX, HP-UX, BSD, Windows, Mac and VMware ESX.

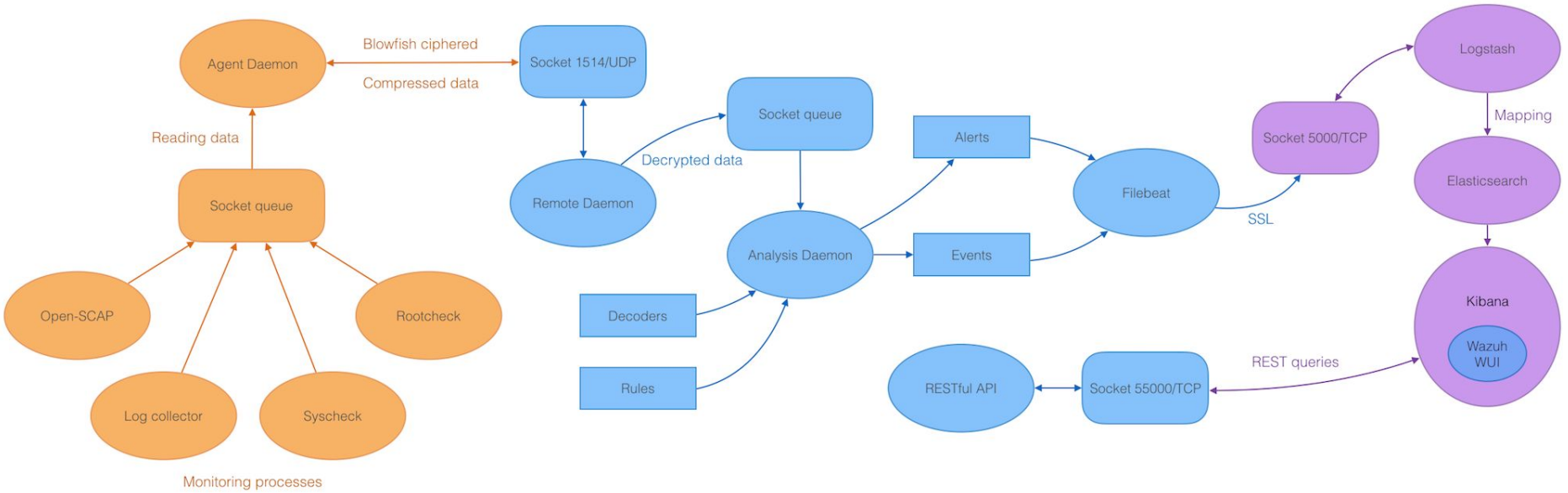


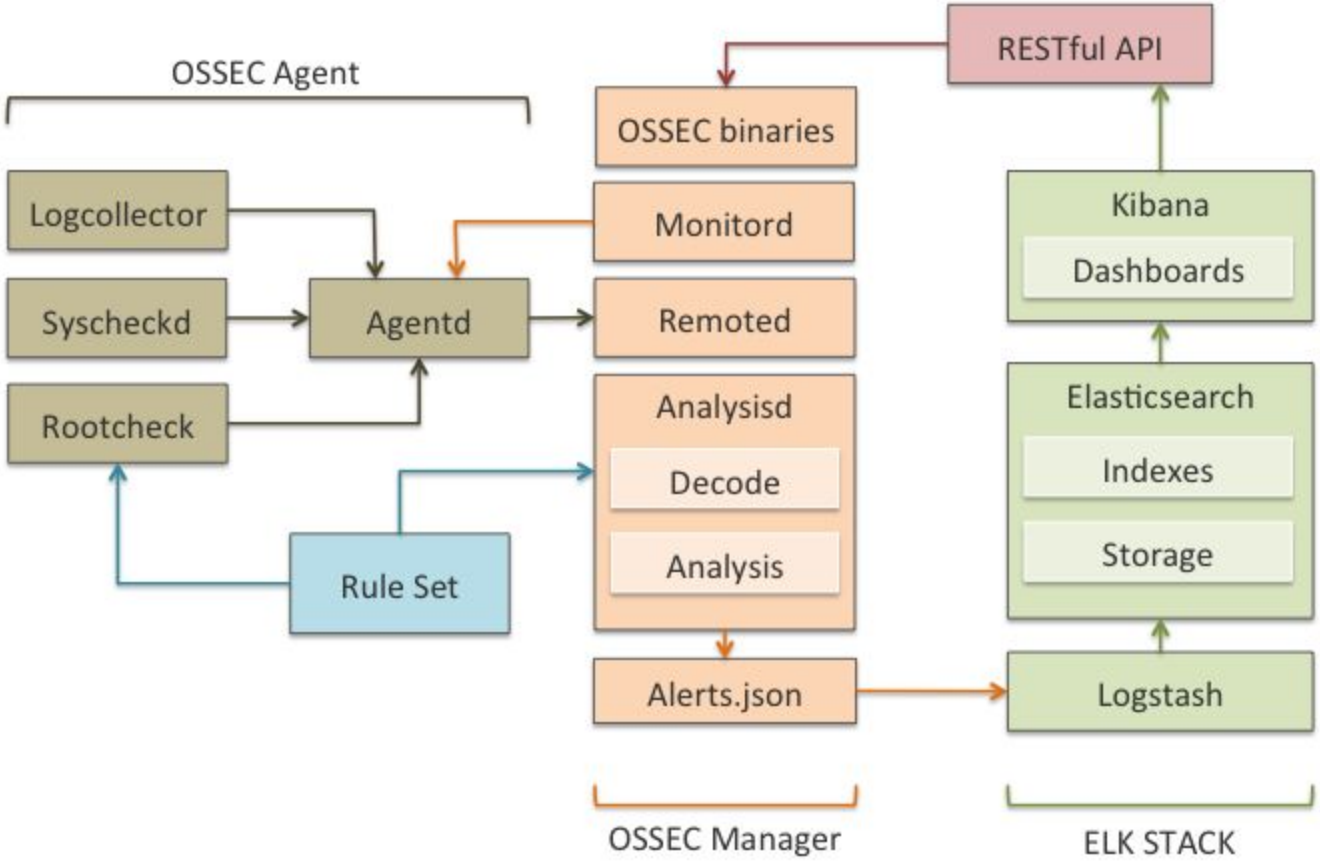

OSSEC Agents
OSSEC Server
Logs
Alerts via syslog
logstash
Web Browser
kibana
Queries
Log analysis
elasticsearch
Log data

Agent processes

Manager processes

Elastic processes



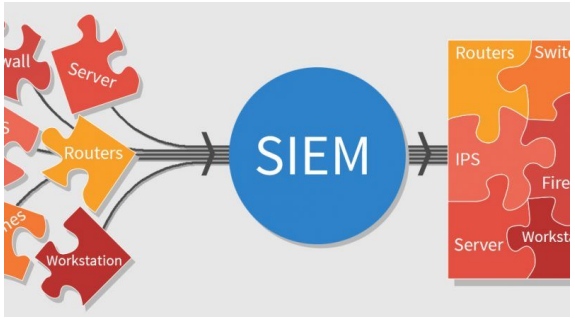

OSSEC Agent
Logcollector
Syscheckd
Rootcheck
Agentd
Rule Set
OSSEC binaries
Monitord
Remoted
Analysisd
Decode
Analysis
Alerts.json
OSSEC Manager
RESTful API
Kibana
Dashboards
Elasticsearch
Indexes
Storage
Logstash
ELK STACK

Top SIEM Vendors

●●●● BEST ●●● VERY GOOD ●● GOOD ● FAIR

SIEM VENDOR	THREATS BLOCKED	SOURCES INGESTED	PERFORMANCE	VALUE	IMPLEMENTATION	MANAGEMENT	SUPPORT	SCALABILITY
splunk> ES	●●●●	●●●	●●●	●●●	●●	●●●	●●	●●●
LogRhythm ENTERPRISE	●●●	●●●●	●●●	●●	●●●	●●●	●●●	●●
USM	●●●	●●●	●●●	●●●●	●●●	●●	●●	●●●
MICRO FOCUS ArcSight	●●	●●●	●●●	●●	●●●	●●●●	●●	●●●
MICRO FOCUS Sentinel	●●	●●	●●	●●●	●●●	●●●	●●	●●●
McAfee ESM	●●●	●●●	●●●	●●●	●●	●●	●●●	●●●
Trustwave SIEM	●●●	●●●	●●●	●●●	●●	●●●	●●	●●●●
IBM QRadar	●●●	●●●	●●●●	●●●	●●	●●●	●●●	●●●
RSA NetWitness	●●	●●	●●●	●●	●●	●●	●●●	●●●
solarwinds LEM	●●	●●●	●●	●●	●●●●	●●	●●●	●●

SOURCE: **eSecurityPlanet.com**



Existe una gran variedad de opciones para adoptar una solución SIEM.

El soporte y mantenimiento de las limitaciones de una solución Open Source difiere frente soluciones propietarias basadas en licencias.

En el mercado actual encontramos soluciones libres o basadas en un proveedor, disponiendo actualmente de las siguientes opciones mayoritarias:

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (August 2016)

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (December 2017)

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (December 2018)

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Security Onion

- https://securityonion.net/
- https://github.com/Security-Onion-Solutions/security-onion/wiki
- https://blog.securityonion.net/

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

AlienVault Open Source SIEM (OSSIM)

https://www.alienvault.com/products/ossim

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

EMC RSA Security Analytics - Centro de operaciones de seguridad avanzado.

http://spain.emc.com/security/security-analytics/security-analytics.htm

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

HP ArcSight Enterprise Security Manager (ESM)

http://www8.hp.com/es/es/software-solutions/arcsight-esm-enterprise-security-management/

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

IBM Security QRadar SIEM

https://www.ibm.com/es-es/marketplace/ibm-qradar-siem

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

LogRhythm Security Intelligence Platform

https://es.logrhythm.com/products/threat-lifecycle-management-platform/

https://es.logrhythm.com/

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

McAfee Enterprise Security Manager

https://www.mcafee.com/es/products/enterprise-security-manager.aspx

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

SolarWinds Log & Event Manager

https://www.solarwinds.com/es/siem-security-information-event-management-software

https://www.solarwinds.com/es/log-event-manager-software

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Splunk Enterprise

https://www.splunk.com/en_us/software/enterprise-security.html

https://www.splunk.com/es_es/products/splunk-enterprise.html

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Lookwise Enterprise Manager

https://www.s21sec.com/es/lookwise-enterprise-manager/

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Graylog 2

https://www.graylog.org/

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

LOGanalize

http://loganalyzer.adiscon.com/

SIEM... Otras opciones **alternativas** para componentes compatibles:

Plataforma de despliegue y gestión de sistemas de contenedores Docker y Kubernetes.

https://rancher.com/

https://github.com/rancher/rancher

SIEM... Otras opciones **alternativas** para componentes compatibles:

Middleware de mensajería para la negociación de mensajes de código abierto.

- https://www.rabbitmq.com/
- https://www.rabbitmq.com/getstarted.html
- https://www.rabbitmq.com/documentation.html
- https://www.rabbitmq.com/download.html
- https://github.com/rabbitmq/rabbitmq-tutorials

SIEM... Otras opciones **alternativas** para componentes compatibles:

Sistema para almacenar y compartir información relacionada con los resultados de las pruebas de penetración.

https://dradisframework.com/ce/

https://dradisframework.com/ce/documentation/

https://github.com/dradis/dradis-ce

SIEM... Otras opciones **alternativas** para componentes compatibles:

Aplicación para el inventariado, auditoría, documentación y gestión de redes.

https://www.open-audit.org/

https://github.com/Opmantek/open-audit

https://community.opmantek.com/display/OA/Home

SIEM... Otras opciones **alternativas** para componentes compatibles:

Soluciones automáticas de informes, logs y alertas.

https://www.skedler.com/

https://www.skedler.com/documentation/

SIEM... Otras opciones **alternativas** para componentes compatibles:

Gestión y compartición inteligencia de amenazas.

https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld

https://github.com/PaloAltoNetworks/minemeld

https://github.com/PaloAltoNetworks/minemeld/wiki

SIEM... Otras opciones **alternativas** para componentes compatibles:

Análisis y visualización de métricas en tiempo real.

https://grafana.com/

https://github.com/grafana/grafana

See what **SIEMonster** can do **Watch Demo**

SIEMonster Features

Human Based Behavior

SIEMonster now provides Human Based behavior correlation options to enrich your alerts and minimize false positives.

Learn more

Threat Intelligence

SIEMonster provides real time Threat intelligence with commercial or opensource feeds to stop real time attacks.

Learn more

Deep Learning

Using Machine Learning, Human Based Behavior analytics watch SIEMonster Deep Learning kill the attacks automatically.

Learn more

SMB & Enterprise

Whether you're a SMB, Enterprise or Managed Security Service Provider, SIEMonster has the scalable solution for you.

Learn more

Cloud or Onsite

SIEMonster allows you to run, onsite in a VM, Bare metal or any of the Cloud providers such as Amazon, GCP or Azure.

Learn more

SIEMonster V3.0 **out now** **Download Now**

What is SIEMonster.
Introduction video on what
is SIEMonster.

SIEMonster OSINT.
SIEMonsters Open Source integrated Threat Intelligence.

SIEMonster Demo.
Video on how the dashboard and other elements work.

SMB-Enterprise Demo.
A detailed walkthrough video about SIEMonster V4.

SIEMonster https://siemonster.com/

https://kb.siemonster.com/help/get-started-with-knowledgeowl

SIEMonster V3 Virtual Machine Build Guide

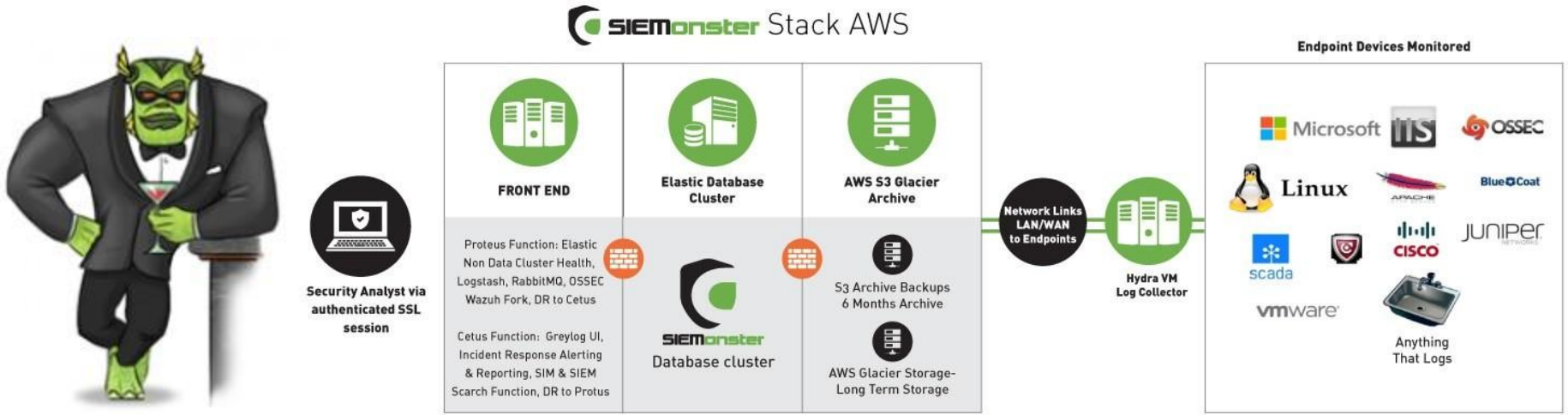
https://kb.siemonster.com/help/siemonster-v3-virtual-machine-build-guide

https://dyzz9obi78pm5.cloudfront.net/app/image/id/5a6d75cd8e121c965f7a7a8c/n/siemonster-v3-vm-build-guide-v18.pdf

SIEMonster https://siemonster.com/

SIEMonster Operations Guide https://kb.siemonster.com/help/siemonster-operations-guide

https://dyzz9obi78pm5.cloudfront.net/app/image/id/5a5c82378e121c3358a273cf/n/siemonster-v3-operations-guide-v11.pdf



SIEMonster https://siemonster.com/

SIEMonster High Level Design

https://kb.siemonster.com/help/siemonster-high-level-design

https://dyzz9obi78pm5.cloudfront.net/app/image/id/5a5bfa2d6e121cc31ab45a9d/n/siemonster-v3-high-level-design-v14.pdf

Contact Us Login

Welcome to the SIEMonster Knowledge Base

Search for articles...

Documents | Videos | Wishlist

Popular Articles

SIEMonster V3 Virtual Machine Build Guide
SIEMonster High Level Design
SIEMonster Operations Guide
SIEMonster V3 Bare Metal Build Guide
SIEMonster Version 3 DIY VM Install Video Step by Step
See more...

New Articles

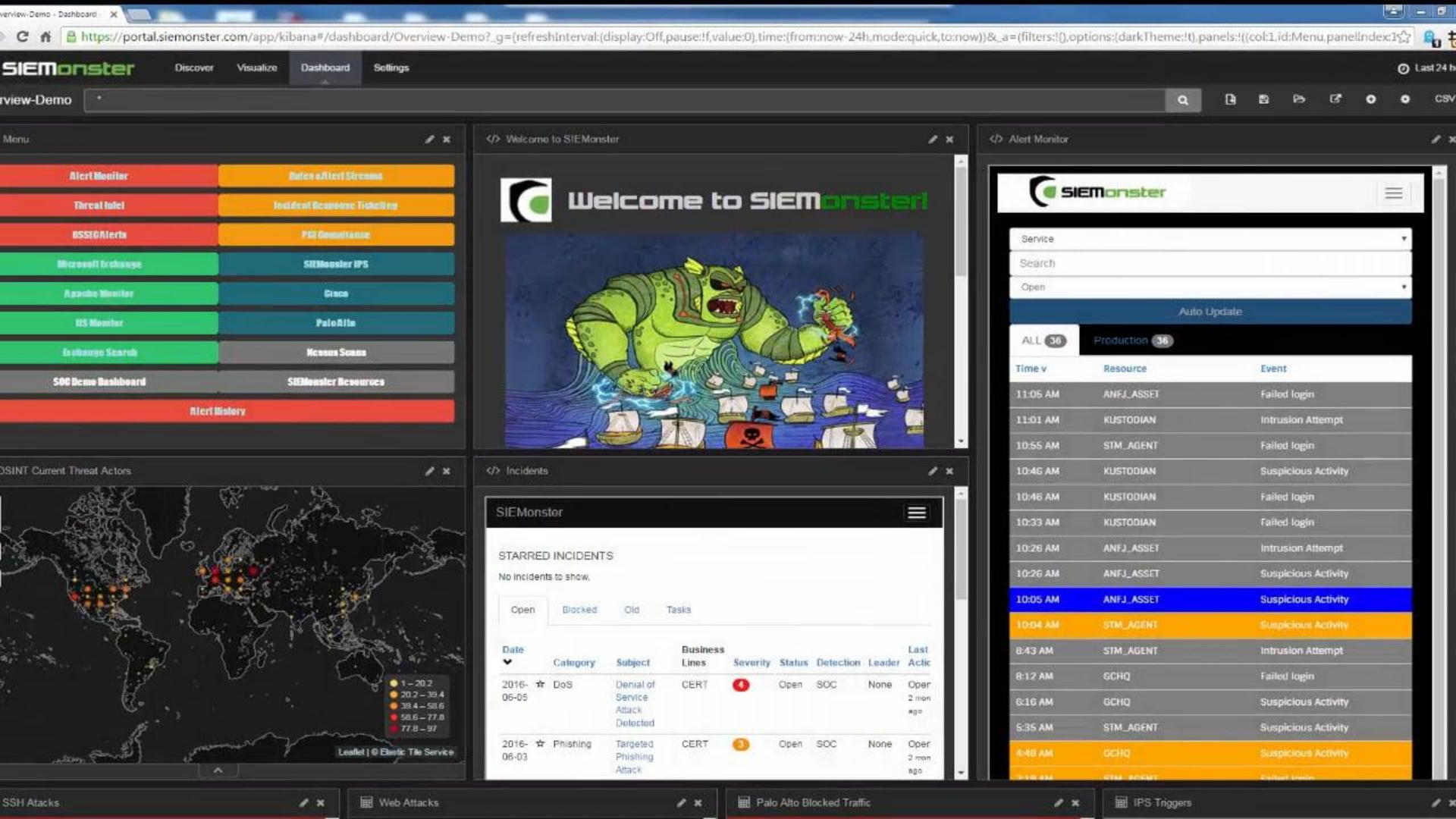
SIEMonster Version 3 DIY VM Install Video Step by Step
SIEMonster V3 Amazon AWS Build Guide
SIEMonster V3 VM Image Builder
SIEMonster V3 Bare Metal Build Guide
Wishlist via Trello
See more...

Updated Articles

SIEMonster Version 3 DIY VM Install Video Step by Step
SIEMonster V3 Virtual Machine Build Guide
SIEMonster V3 Bare Metal Build Guide
SIEMonster V3 Amazon AWS Build Guide
SIEMonster High Level Design
See more...

SIEMonster https://siemonster.com/ Funciones de los monstruos:

- **Makara**: Planificación y coordinación del Rancher (Plataforma de software de código abierto que permite ejecutar contenedores en producción a las organizaciones), aplicación front-end web, servidor NFS y análisis y procesamiento de registro de eventos desde la cola de mensajes RabbitMQ antes de pasar al nodo ES Client 1 Elastic.
- **Proteus** (Proteo): Ingerir y procesar datos de endpoint entrantes y reenviar al intermediario de mensajes RabbitMQ y proporcionar alojamiento para cualquiera de las aplicaciones agrupadas. Recibe los registros de los Windows, Linux, aplicaciones y hardware que proporciona el syslog. Los agentes proporcionan encriptación TLS / SSL usando diferentes certificados.
- **Capricorn**: Elastic Client Node 2 y proporciona alojamiento para cualquiera de las aplicaciones agrupadas.
- **Kraken**: Cluster Node 1 Elastic que almacena todos sus datos SIEM a largo plazo en la base de datos proporcionando redundancia para Tiamat Cluster Node 2.
- **Tiamat**: Cluster Node 2 Elastic que almacena todos sus datos SIEM a largo plazo en la base de datos proporcionando redundancia para Kraken Cluster Node 1.
- **Ikuturso** (Iku Turso): Es un sensor de red alejado de SIEM que se encuentra en una DMZ o borde de red, ejecutando BRO, LOGSTASH, RabbitMQ, Suricata con la capacidad de bloquear el tráfico conocido utilizando Threat Intelligence. También proporciona capacidades forenses de ataques conocidos con aplicaciones e inspección de paquetes de red.
- **Hydra** (Hydra of Lerna): Servidor de recopilación de registros en el sitio del cliente que envía de forma segura los datos recopilados a SIEMonster MSSP para su procesamiento y almacenamiento.

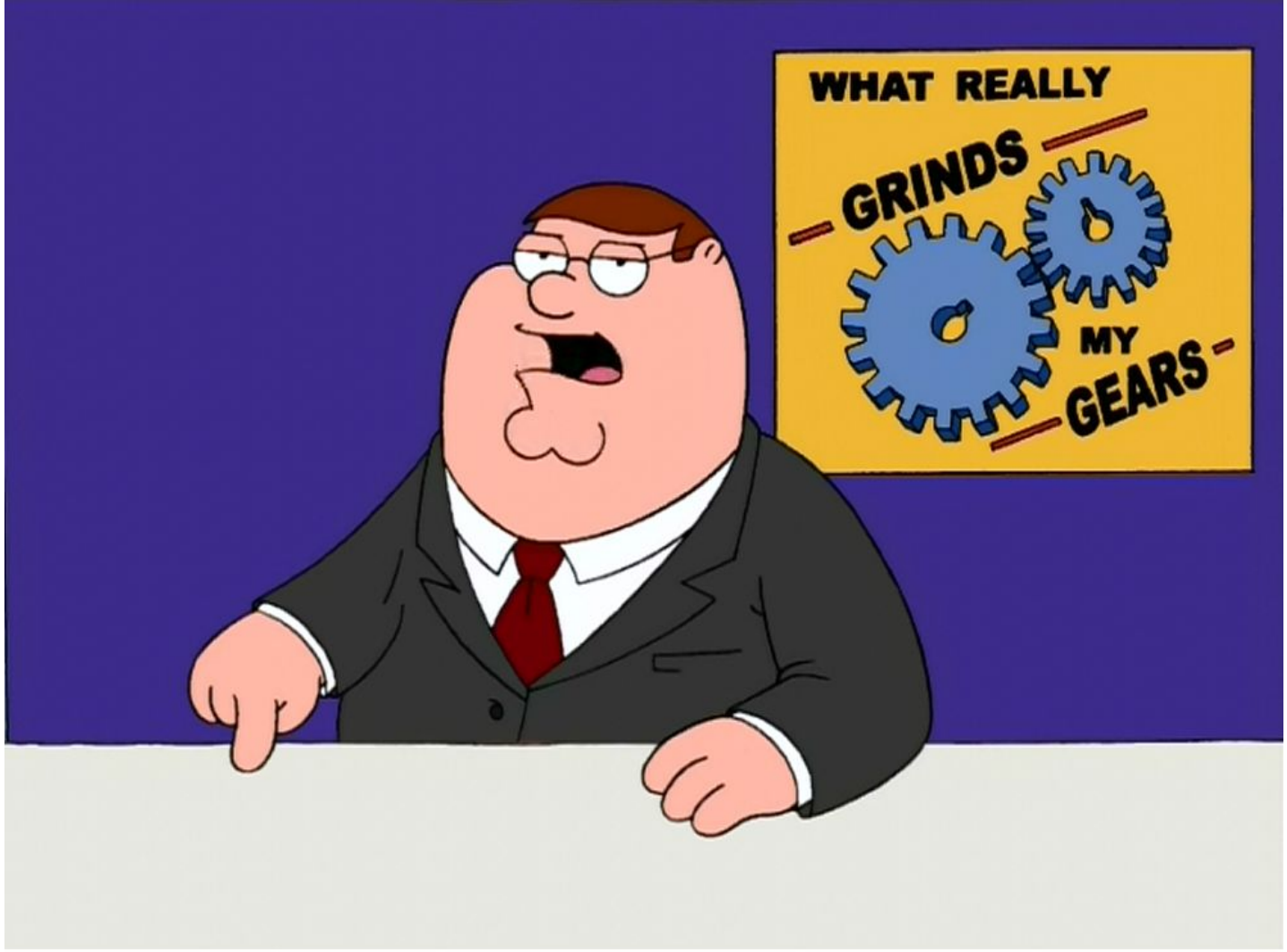

SIEMonster
Discover
Visualize
Dashboard
Settings
Menu
Alert Monitor
Threat Intel
Palo Alto Alerts
Microsoft Exchange
Apache Monitor
IIS Monitor
Exchange Search
SOC Demo Dashboard
Alert History
Palo Alto IPS
Cisco
Nessus Scans
SIEMonster Resources
Welcome to SIEMonster
OSINT Current Threat Actors
Incidents
SIEMonster
STARRED INCIDENTS
No incidents to show.
Open
Blocked
Old
Tasks
Date
Category
Subject
Business Lines
Severity
Status
Detection
Leader
Last Actic
2016-06-05
DoS
Denial of Service Attack Detected
CERT
Open
SOC
None
2016-06-03
Phishing
Targeted Phishing Attack
CERT
Open
SOC
None
Service
Search
Open
Auto Update
ALL 36
Production 36
Time v
Resource
Event
11:05 AM
ANFJ_ASSET
Failed login
11:01 AM
KUSTODIAN
Intrusion Attempt
10:55 AM
STM_AGENT
Failed login
10:46 AM
KUSTODIAN
Suspicious Activity
10:46 AM
KUSTODIAN
Failed login
10:33 AM
KUSTODIAN
Failed login
10:26 AM
ANFJ_ASSET
Intrusion Attempt
10:26 AM
ANFJ_ASSET
Suspicious Activity
10:05 AM
ANFJ_ASSET
Suspicious Activity
10:04 AM
STM_AGENT
Suspicious Activity
8:43 AM
STM_AGENT
Intrusion Attempt
8:12 AM
GCHQ
Failed login
6:16 AM
GCHQ
Suspicious Activity
5:35 AM
STM_AGENT
Suspicious Activity
4:48 AM
GCHQ
Suspicious Activity
SSH Attacks
Web Attacks
Palo Alto Blocked Traffic
IPS Triggers

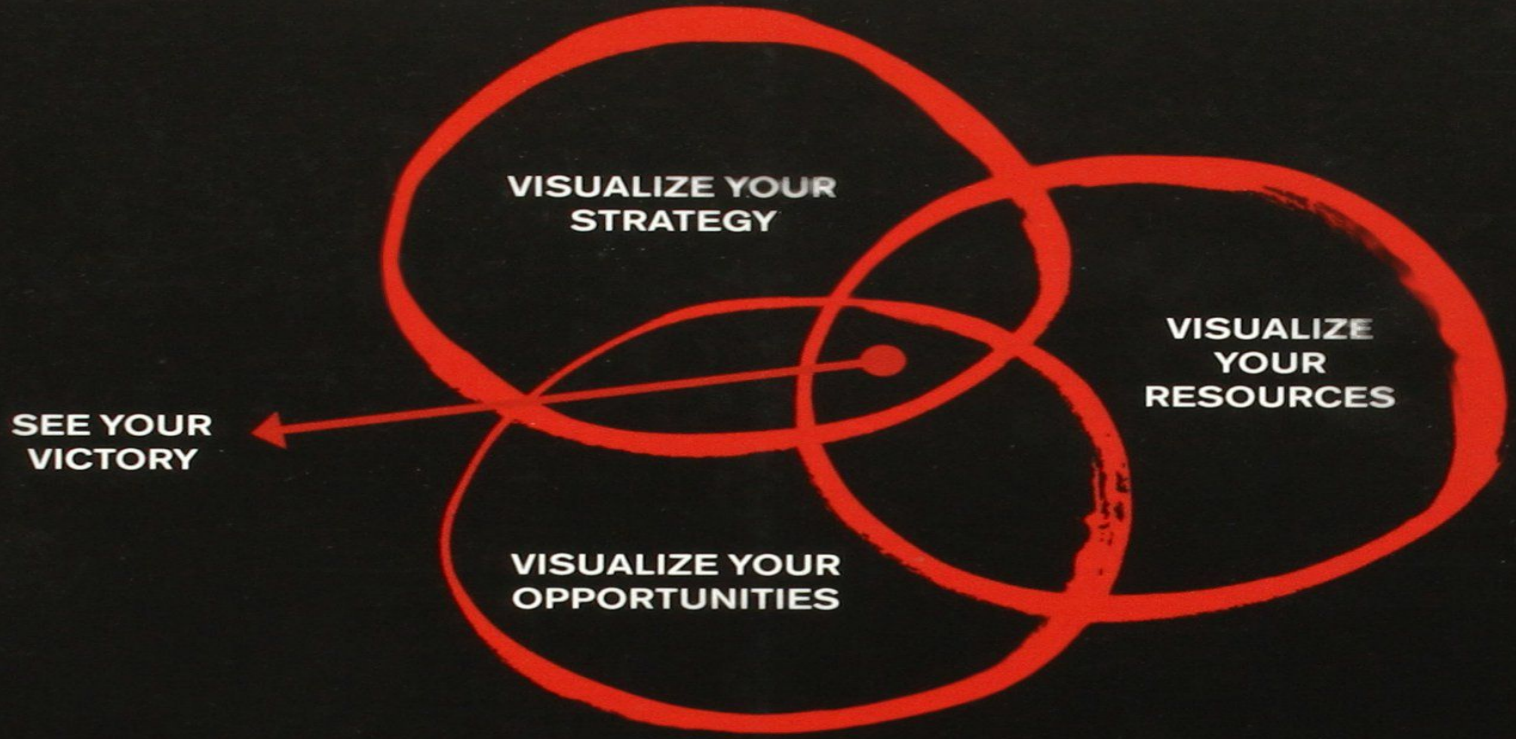
SIEMonster

PRODUCTS DOWNLOADS SUPPORT CONTACT SALES NEWS PARTNERS ABOUT US

You can have your very own SIEMonster

Send me a Monster! **Purchase Now**


WHAT REALLY
GRINDS
MY
GEARS



THE ART OF WAR has been a game plan to success for more than 800 years. THE ART OF WAR VISUALIZED is its total transformation for the 21st century. Use it whenever there's something worth fighting for.

BIBLIOTECA INGENIOS

EL ARTE DE LA GUERRA

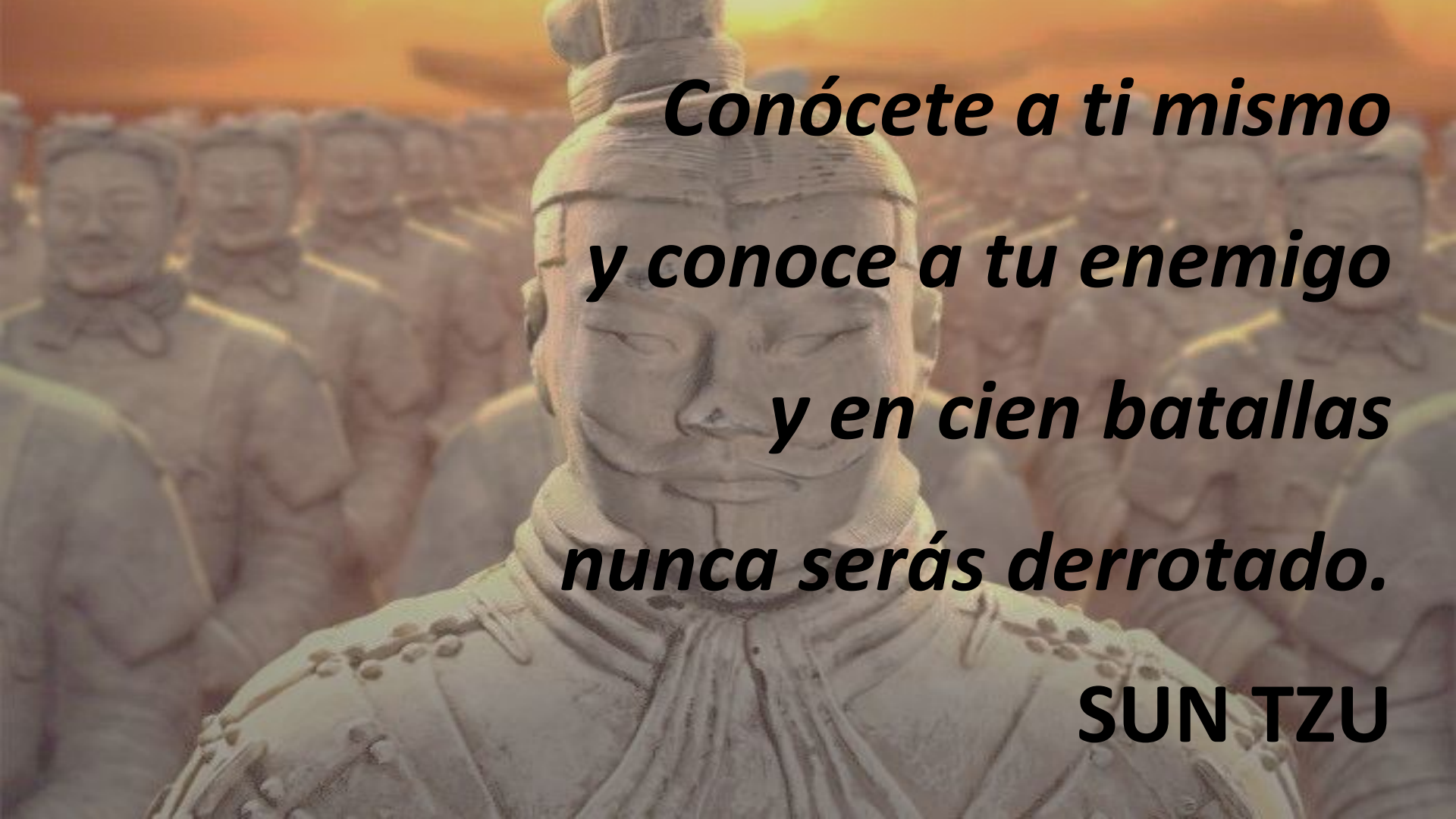
SUN TZU

LAS VICTORIAS DE LOS BUENOS GUERREROS NO SE DEBEN A LA SUERTE, SINO A HABERSE SITUADO PREVIAMENTE EN POSICIÓN DE GANAR CON SEGURIDAD, IMPONIÉNDOSE SOBRE LOS QUE YA HAN PERDIDO DE ANTEMANO.

SUN TZU

EL ARTE DE LA GUERRA

Biblok


Conócete a ti mismo
y conoce a tu enemigo
y en cien batallas
nunca serás derrotado.
SUN TZU