SIEM con Elastic

Junio 2021

Nuestro ADN

Training academy

Formación oficial
y píldoras formativas
especializadas

Partners Top

Máximo nivel de
certificación en
Partnerships

Certificaciones

Certificaciones
tecnológicas
premium

24/7

Gestión y
monitorización
24/7

4 Sedes

Barcelona 22@
Barcelona PTV
Madrid
Girona

Expertos

En diseño e
integración de soluciones
tecnológicas

Equipo

de +70 personas
en la plantilla de
Davinci Group

Crecimiento

Crecimientos
sostenidos anuales
de + 25%

Tecnologías

+150 aplicadas,
desarrolladas
y open source

Experiencia

20 años de
experiencia en el
sector

Áreas especializadas

Fusionamos el conocimiento entre divisiones tecnológicas
para conseguir una visión global y transversal de cada proyecto

digital platforms

Gestionamos el conocimiento y desarrollamos plataformas digitales seguras en la nube.

ackstorm davinci cloud

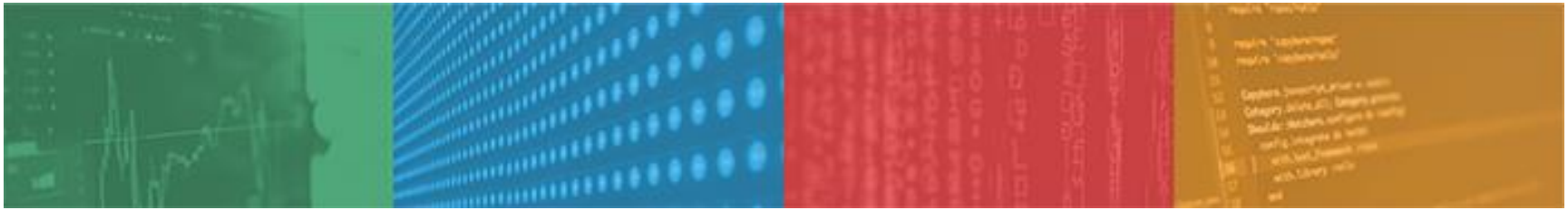
Arquitectos Cloud: diseñamos, implementamos y gestionamos plataformas en Cloud público.

cyber & cloud security

Convertimos la seguridad en el principal aliado para garantizar agilidad y resiliencia.

data analytics & enterprise search

Procesamos y preparamos la información para hacerla práctica, gestionable y analizable.



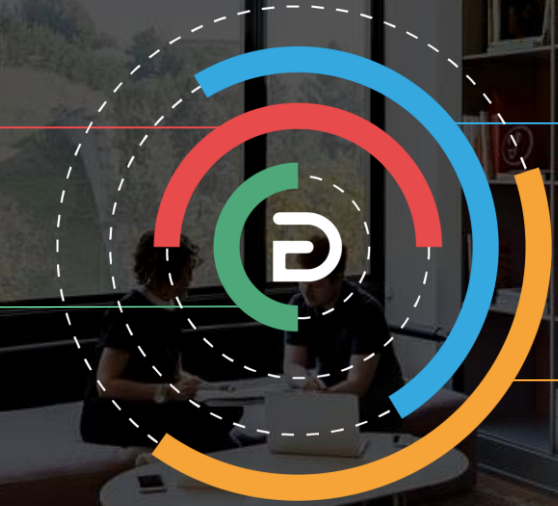
¿Por qué nos escogen?

Calidad de los proyectos

Perspectiva integral

Equipo experto

Confianza de nuestros clientes



Secure Digital Cloud Platforms

davinci group

Principal Premium Partners

Azure Partner

Google Premier Partner

IBM Cloud

AWS Advanced

Elastic Advanced Reseller

IBM Security

Kaspersky Platinum Partner

Check Point Certified MSSP

Principales clientes

Industria

edebé

CIRSA

CELSA GROUP

in-Store Media
Right place. Right time.

Lavinia

macmillan education

Applus IDIADA

GOLDCAR

COSTAISA

FC Barcelona

Nintendo

Basílica de la Sagrada Família

FLUIDRA

MECALUX

SERHS

RBA

Pepe Jeans
LONDON

IBEROSTAR
HOTELS & RESORTS

vueling

Admin. Pública

Ajuntament de Barcelona

Bilbao

Ajuntament de Gavà

Generalitat de Catalunya

TMB Transports Metropolitans de Barcelona

madriddigital
Agencia para la Administración Digital de la Comunidad de Madrid

Ajuntament de L'Hospitalet

Diputació de Girona

Diputació Tarragona

Barcelona Activa

cesicat

Consejo General del Poder Judicial

CENDOJ
CENTRO DE DOCUMENTACIÓN JUDICIAL

IMI
Institut Municipal d'Informàtica

BASE
GESTIÓ D'INGRESSOS

Port de Barcelona

Diputació Barcelona

Banca

Sabadell

BANCO DE ESPAÑA
Eurosistema

mediolanum
BANCO

TSB

Farma

REIG JOFRE

Agència de Salut Pública

medichem

ORDESA

Retail

Sprinter

SALVADOR ESCODA S.A.

mr wonderful

VIENA

esdemarca

eDreams ODIGEO

MANGO

davinci group

davinci group

Elastic Security

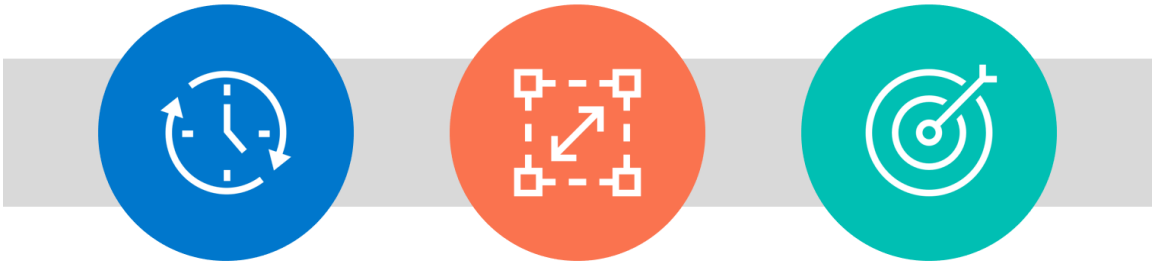
Search, Observe, Protect

Elastic

Motor de Búsqueda con capacidades analíticas

- Grandes volúmenes de información
- Escalable horizontalmente
- Tiempo Real (ingesta, consulta)
- Consultas y agregaciones con resultados muy precisos de forma muy rápida
- Respuestas relevantes y acordes al criterio de búsqueda

Pilares



3 Soluciones

Elastic Enterprise Search

Elastic Observability

Elastic Security

3 Soluciones proporcionadas por 1 Stack

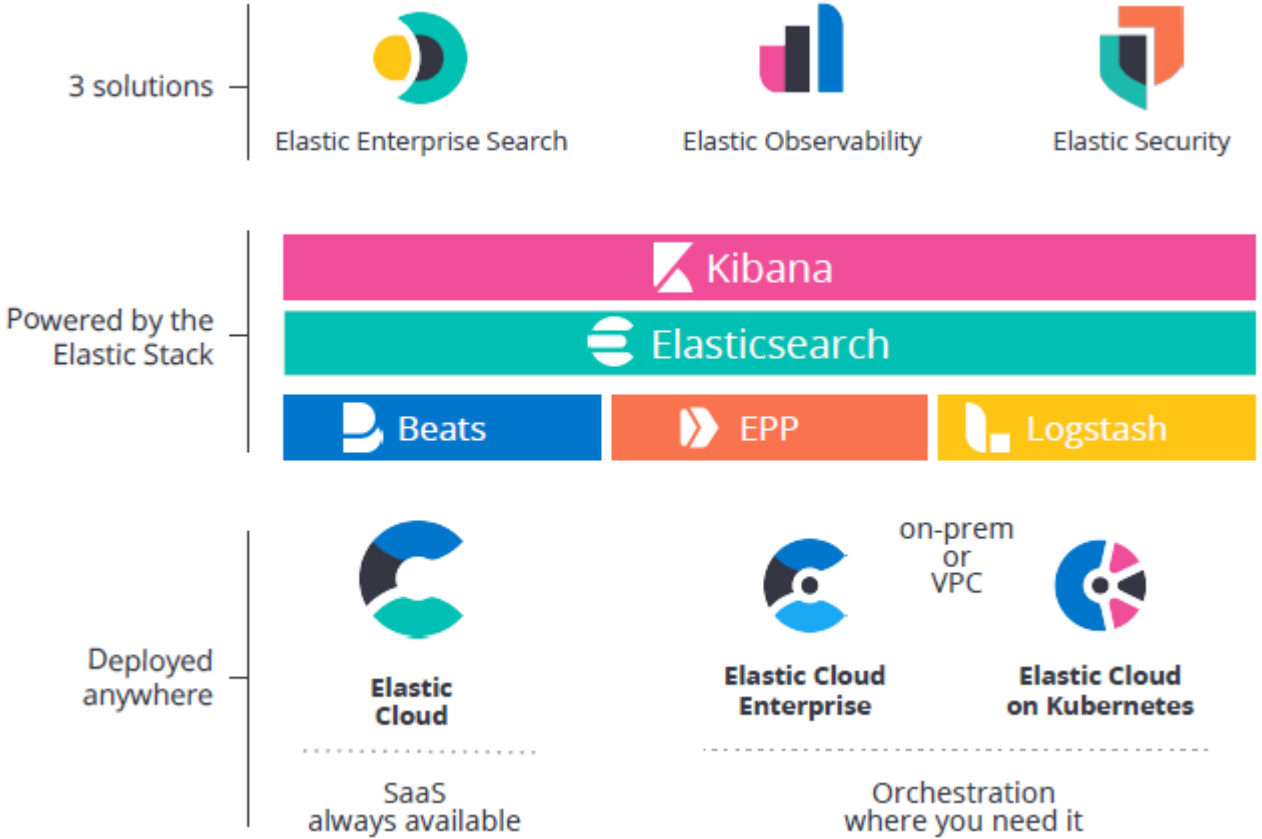
Elastic Enterprise Search

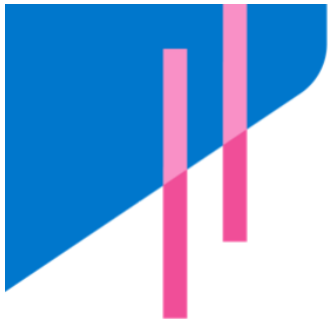
Elastic Observability

Elastic Security

Elastic Stack

Múltiples opciones de despliegue





Search. Observe. Protect.

Casos de Uso

Enterprise Search

- App Search
- Site Search
- Workplace Search

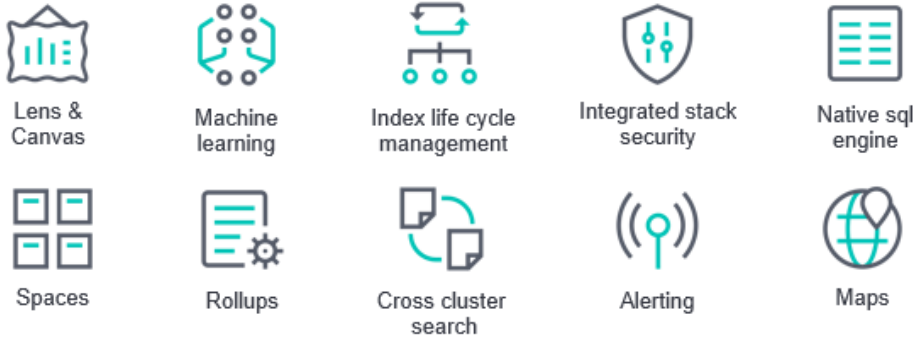
Observability

- Logs
- Metrics
- Service Monitoring
- Application Performance

Security

- SIEM
- Endpoint Security

Elastic Stack



Elastic Security

Search, Observe, Protect

Visibilidad completa de la seguridad en una **única plataforma** abierta, a un **precio asequible**

Elastic Security

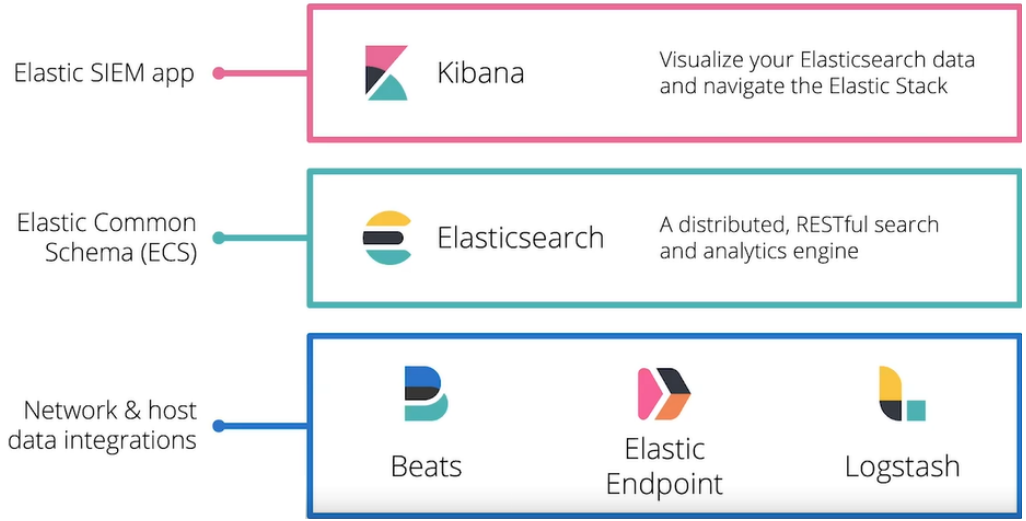
Elastic Security se apoya en las **funcionalidades avanzadas de Elasticsearch** para proporcionarnos lo que mejor sabe hacer: **buscar en tiempo real sobre un gran volumen de información.**

· Objetivo: protección ante amenazas ***(SIEM + Endpoint)*:**

- Prevención
- Detección
- Respuesta a amenazas.

Elastic SIEM

¿Qué es Elastic SIEM?



Elastic SIEM

Elastic Common Schema

Searching *without* ECS	Searching *with* ECS

`src:10.42.42.42`
`OR client_ip:10.42.42.42`
`OR apache2.access.remote_ip:`
`10.42.42.42`
`OR context.user.ip:10.42.42.42`
`OR src_ip:10.42.42.42`
	`source.ip:10.42.42.42`

- **Definición estándar** de un conjunto de campos y objetos a ingestar en Elasticsearch
- Diseñado para ser extendido
- Todos los Elastic **Beats utilizan ECE**
- Permite **analizar diferentes fuentes de datos** de forma cruzada **en un único dashboard**

https://github.com/elastic/ecs

Elastic SIEM

Beats

Host data

FileBeat
Log Files &
Remote Ingest

AuditBeat
Audit Data

WinLogBeat
Window Events

Network data

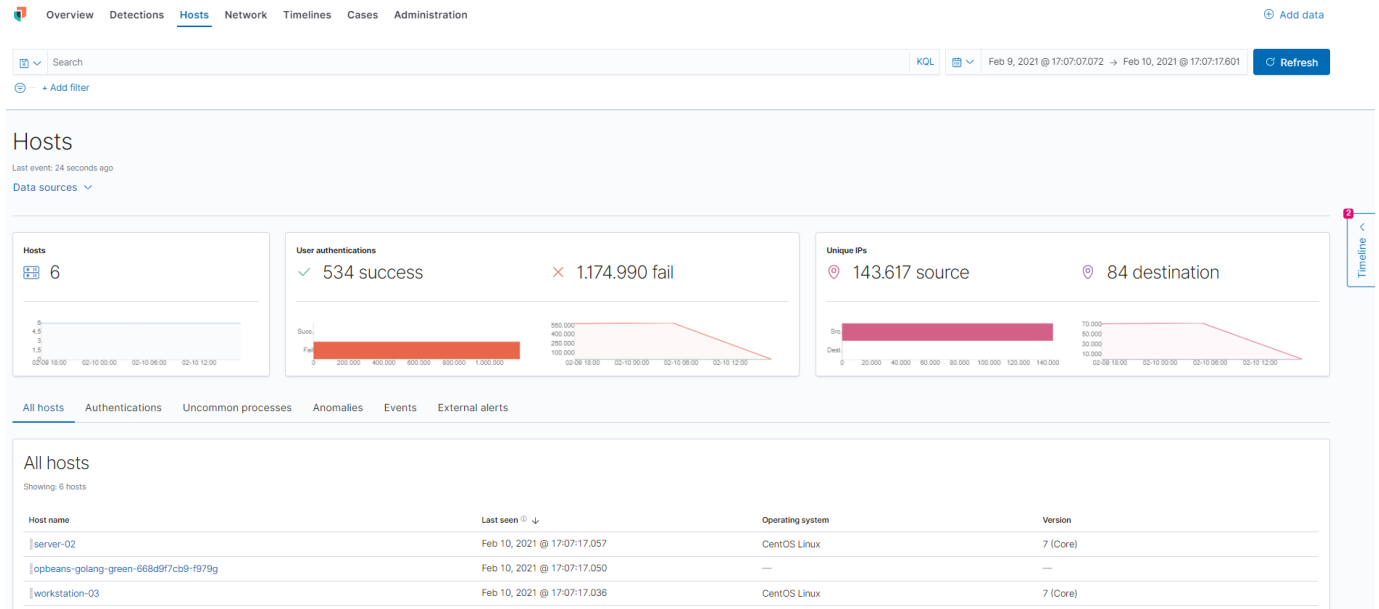
FileBeat
modules

PacketBeat
Network Data

Elastic Data Sources Integration: https://www.elastic.co/es/integrations?solution=security

Elastic SIEM

SIEM App

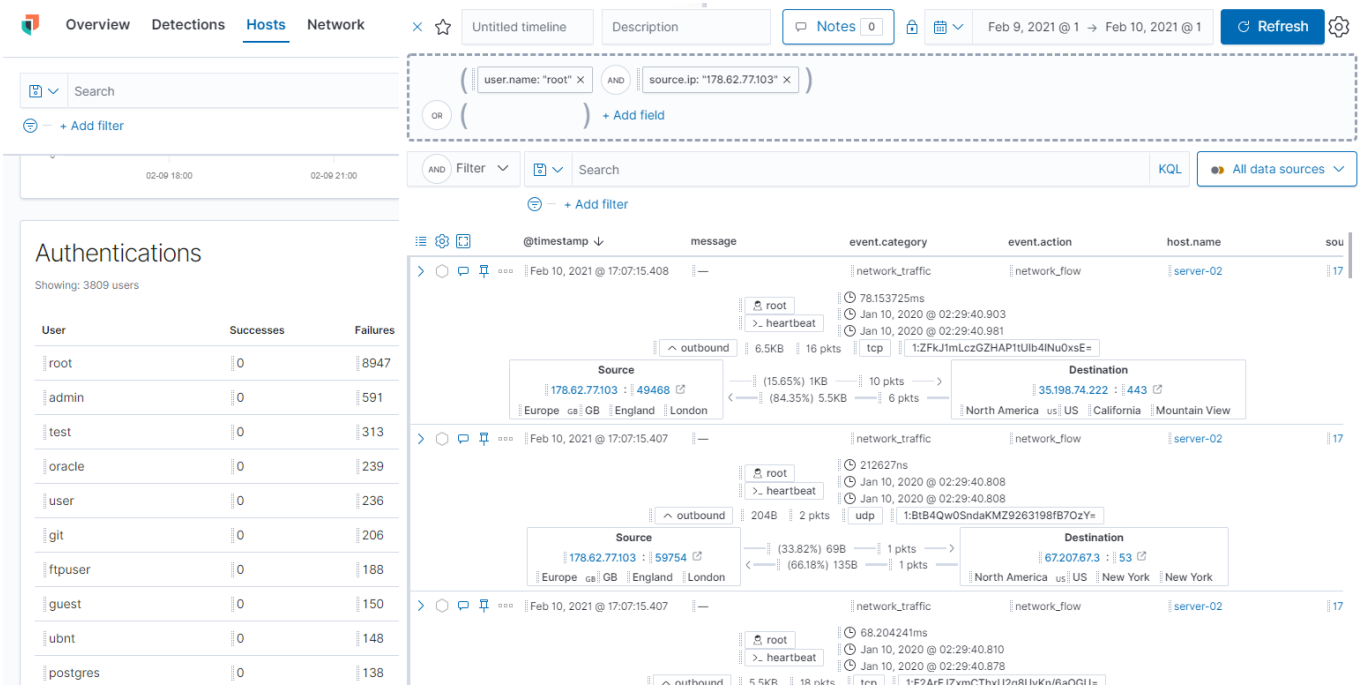


- *Gestión de eventos de seguridad.*
- *Trabajos de investigación.*
- *Creación de incidentes.*
- *Etc*

Elastic SIEM

Timeline

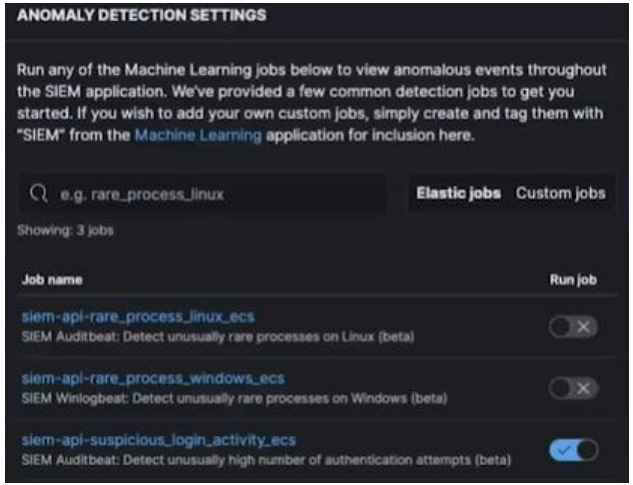
- *Ordenación de eventos.*
- *Filtrado por drag&drop.*
- *Búsquedas en multiples índice.*
- *Comentarios y anotaciones.*
- *Visualización detallada de eventos.*
- *Sin restricciones de retención.*

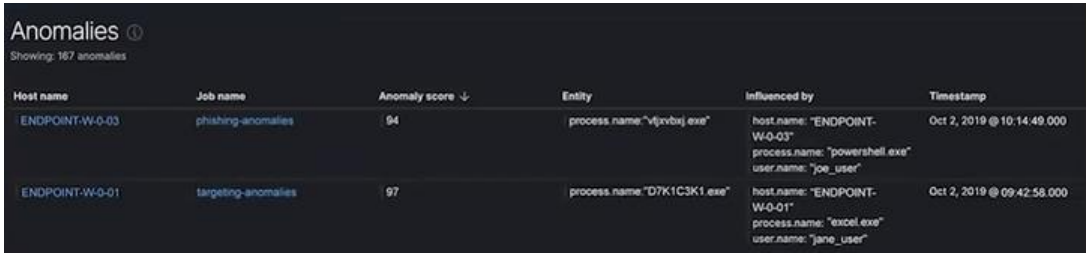


Elastic SIEM

Alertas + Machine Learning

- *Detección no supervisada de anomalías.*
- *Creación de trabajos de ML asociados a nuestro dataset.*
- *Activación de trabajos preconfigurados.*



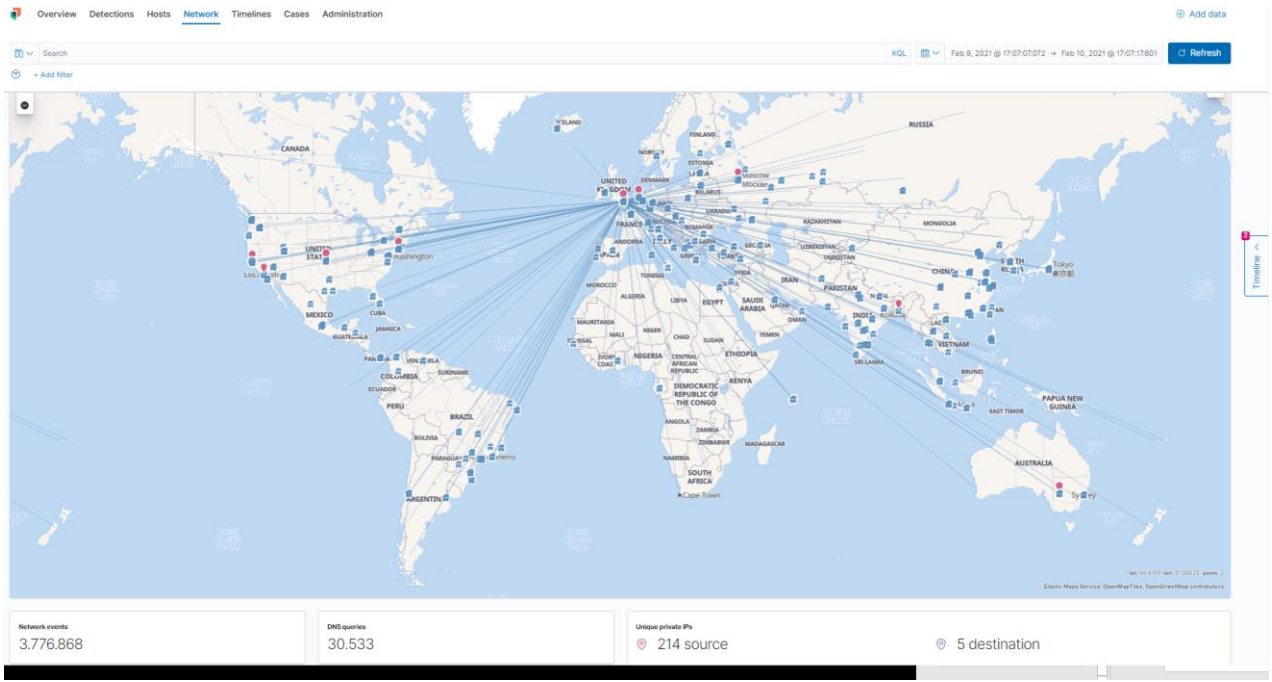


Elastic SIEM

Maps

· *Geolocalización datos.*

· *Interactivo.*



Elastic Security

¿Licencia?

Gratuita / Oro / Platino / Enterprise

· Licencias basadas en funcionalidad avanzada y soporte del fabricante.

· Sin límite en número de agentes.

· Coste según dimensionamiento clúster de Elasticsearch.

https://www.elastic.co/es/pricing/
https://www.elastic.co/es/subscriptions

¿Necesidades AOC?

- ¿Se ha utilizado previamente Elastic para algún caso de uso?
- ¿Se prevé utilizar Elastic Stack para SIEM?
- ¿Se tiene identificada alguna necesidad actualmente?
- ¿Objetivo de cumplimiento de normativas? (Retención de datos, etc)
- ¿Tecnologías a tener en cuenta?
- ¿Se dispone de datos de negocio a incorporar en cuadros de mando?

GRACIAS