



Secure Digital Cloud Platforms

## 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

Equipo experto

Perspectiva integral

Confianza de nuestros clientes

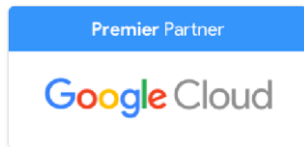


Secure Digital Cloud Platforms

# 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



## Admin. Pública



## Banca



## Farma



## Retail





# Elastic Security

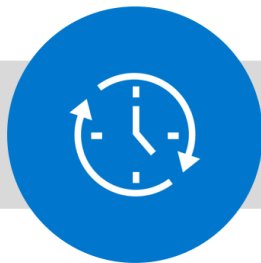
Search, Observe, Protect

## Pilares

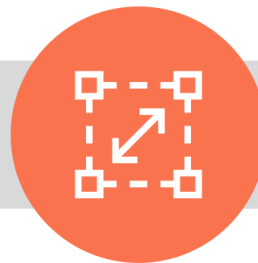
# Elastic

### 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



Velocidad



Escalabilidad



Relevancia



## 3 Soluciones



**Elastic Enterprise Search**



**Elastic Observability**



**Elastic Security**

## 3 Soluciones proporcionadas por 1 Stack



**Elastic Enterprise Search**



**Elastic Observability**



**Elastic Security**

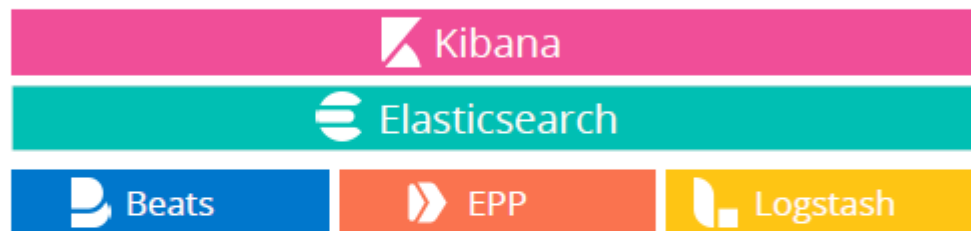


**Elastic Stack**

## Múltiples opciones de despliegue



Powered by the  
Elastic Stack



Deployed  
anywhere





**Search. Observe. Protect.**



## Enterprise Search

- App Search
- Site Search
- Workplace Search

## Observability

- Logs
- Metrics
- Service Monitoring
- Application Performance

## Security

- SIEM
- Endpoint Security

## Elastic Stack



Lens &  
Canvas



Machine  
learning



Index life cycle  
management



Integrated stack  
security



Native sql  
engine



Spaces



Rollups



Cross cluster  
search



Alerting



Maps



## 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 app



Kibana

Visualize your Elasticsearch data  
and navigate the Elastic Stack

Elastic Common  
Schema (ECS)



Elasticsearch

A distributed, RESTful search  
and analytics engine

Network & host  
data integrations



Beats



Elastic  
Endpoint



Logstash



# Elastic SIEM



## Elastic Common Schema

### Searching *without* 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
```

### Searching *with* ECS

```
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**

## Elastic SIEM



### Host data



**FileBeat**  
Log Files &  
Remote Ingest



**AuditBeat**  
Audit Data



**WinLogBeat**  
Window Events

### Network data



**FileBeat**  
modules



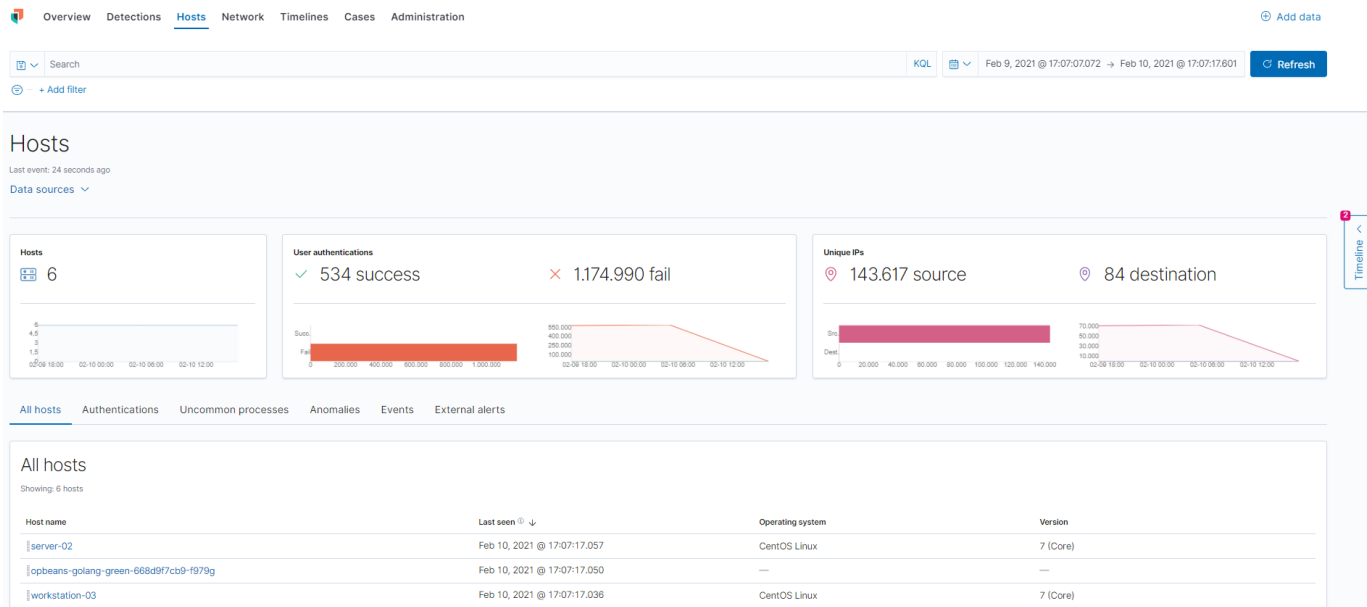
**PacketBeat**  
Network Data

# 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.

Overview Detections **Hosts** Network

Untitled timeline Description Notes 0 Feb 9, 2021 @ 1 → Feb 10, 2021 @ 1 Refresh

Search + Add filter

Authentications

Showing: 3809 users

User	Successes	Failures
root	0	8947
admin	0	591
test	0	313
oracle	0	239
user	0	236
git	0	206
ftpuuser	0	188
guest	0	150
ubnt	0	148
postgres	0	138

Filter AND Filter Search KQL All data sources

message event.category event.action host.name source

Feb 10, 2021 @ 17:07:15.408 network\_traffic network\_flow server-02 17

root heartbeat 78.153725ms Jan 10, 2020 @ 02:29:40.903 Jan 10, 2020 @ 02:29:40.981

outbound 6.5KB 16 pkts tcp 1:2FKJ1mLczGZHAPtUlb4INu0xsE=

Source 178.62.77.103 : 49468 Europe GB England London (15.65%) 1KB 10 pkts (84.35%) 5.5KB 6 pkts

Destination 35.198.74.222 : 443 North America us California Mountain View

Feb 10, 2021 @ 17:07:15.407 network\_traffic network\_flow server-02 17

root heartbeat 212627ns Jan 10, 2020 @ 02:29:40.808 Jan 10, 2020 @ 02:29:40.808

outbound 204B 2 pkts udp 1:BtB4Qw0SndaKMZ9263198fB7OzY=

Source 178.62.77.103 : 59754 Europe GB England London (33.82%) 698 1 pkts (66.18%) 135B 1 pkts

Destination 67.207.67.3 : 53 North America us New York New York

Feb 10, 2021 @ 17:07:15.407 network\_traffic network\_flow server-02 17

root heartbeat 68.204241ms Jan 10, 2020 @ 02:29:40.810 Jan 10, 2020 @ 02:29:40.878

outbound 5.5KB 18 pkts tcp 1:F7&F17vmtT3vRIuKn/RaQGI=

# Elastic SIEM



## Alertas + Machine Learning

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

**ANOMALY DETECTION SETTINGS**

Run any of the Machine Learning jobs below to view anomalous events throughout the SIEM application. We've provided a few common detection jobs to get you started. If you wish to add your own custom jobs, simply create and tag them with "SIEM" from the Machine Learning application for inclusion here.

Q e.g. rare\_process\_linux **Elastic jobs** Custom jobs

Showing: 3 jobs

Job name	Run job
siem-api-rare_process_linux_ecs SIEM Auditbeat: Detect unusually rare processes on Linux (beta)	<input type="checkbox"/>
siem-api-rare_process_windows_ecs SIEM Winlogbeat: Detect unusually rare processes on Windows (beta)	<input type="checkbox"/>
siem-api-suspicious_login_activity_ecs SIEM Auditbeat: Detect unusually high number of authentication attempts (beta)	<input checked="" type="checkbox"/>

**Anomalies** ⓘ  
Showing: 167 anomalies

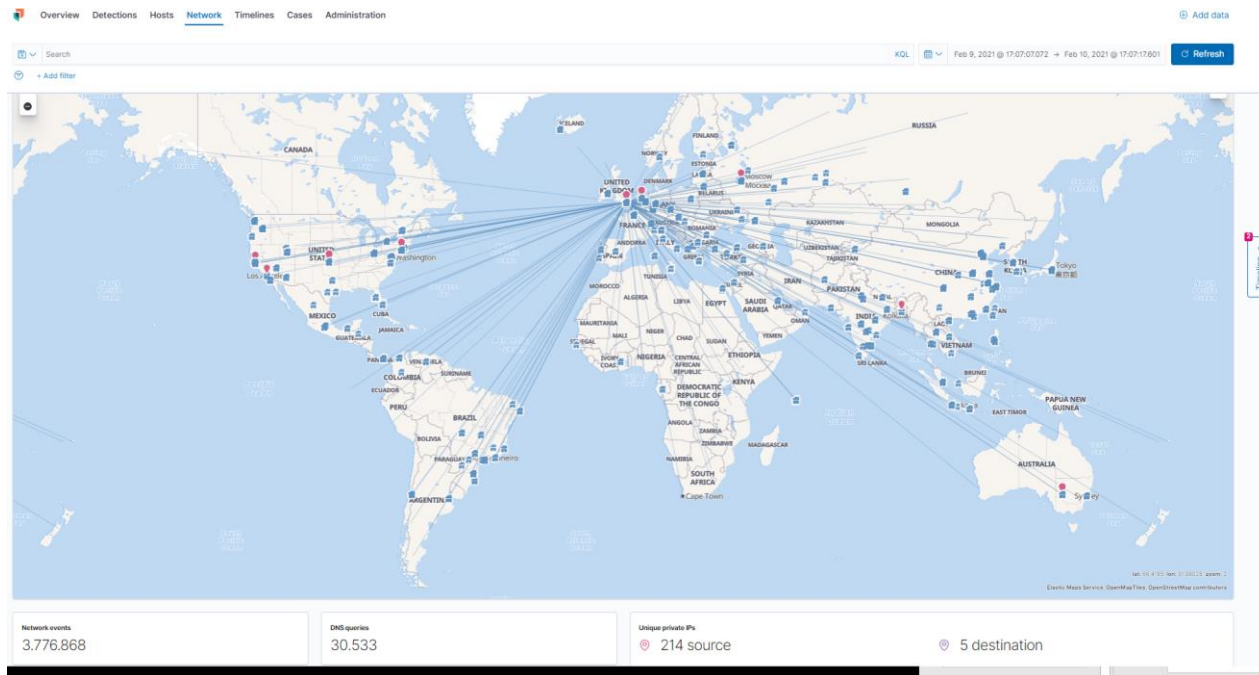
Host name	Job name	Anomaly score ↓	Entity	Influenced by	Timestamp
ENDPOINT-W-0-03	phishing-anomalies	94	process.name:"vjsxbj.exe"	host.name:"ENDPOINT-W-0-03" process.name:"powershell.exe" user.name:"joe_user"	Oct 2, 2019 @ 10:14:49.000
ENDPOINT-W-0-01	targeting-anomalies	97	process.name:"D7K1C3K1.exe"	host.name:"ENDPOINT-W-0-01" process.name:"excel.exe" user.name:"jane_user"	Oct 2, 2019 @ 09:42:58.000

# 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