

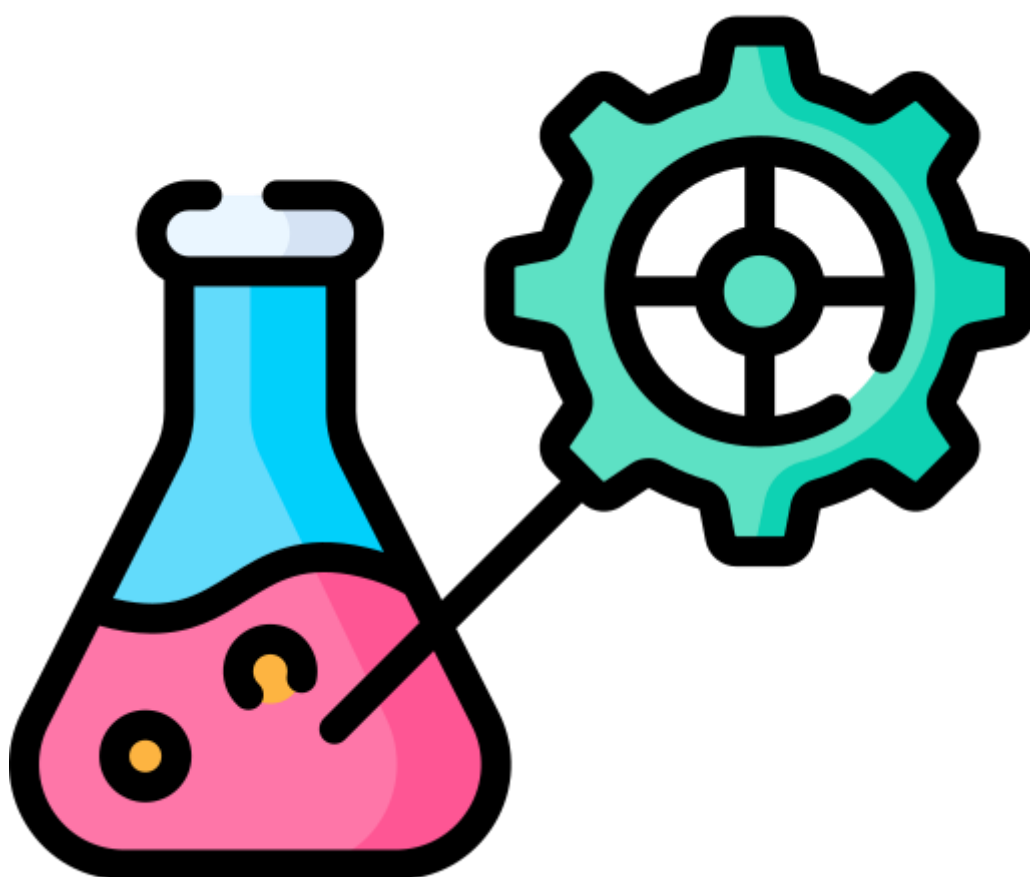


---

# HERRAMIENTA CATALYST

---

PRÁCTICA 3.2



ERIC SERRANO MARÍN  
INCIDENTES DE CIBERSEGURIDAD

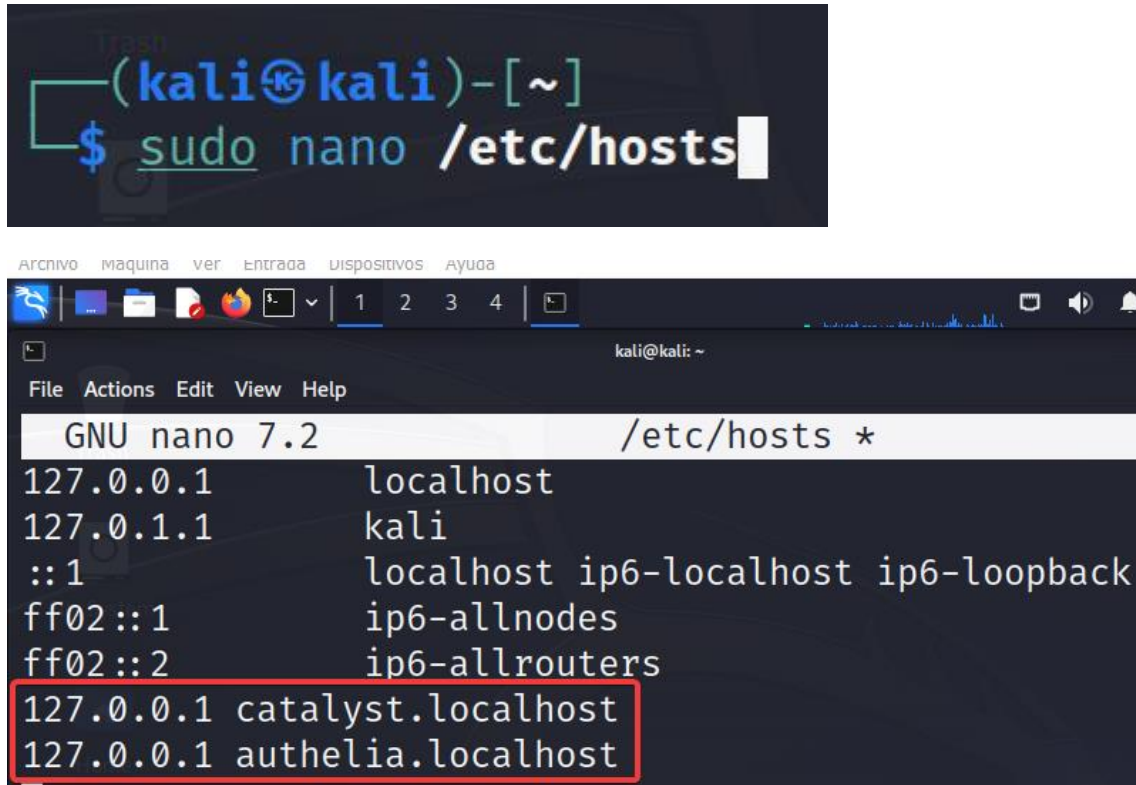
## Contenido

1. Instalación de la herramienta Catalyst .....	2
Vamos a añadir dos líneas de texto al archivo hosts. ....	2
Instalación de Docker.io.....	2
Instalación de Curl. ....	3
Instalación Docker-compose.....	3
Unzip ya lo teníamos instalado. ....	3
Instalación openssl. ....	4
Instalación de sed.....	4
Ahora vamos a descargarnos el script de instalación.....	4
Generar certificado openssl. ....	5
Ejecución del script install_catalyst.sh. ....	5
Error con la ejecución del script.....	5
Accediendo a Catalyst. ....	6
2. Una vez instalada usa la herramienta Catalyst y crea 3 tickets sobre incidentes que hayas catalogado en la actividad 3.1, prestando atención a la taxonomía del incidente descrito. Detalla todos los pasos. ....	9
<b>Ticket 1</b> .....	9
<b>Ticket 2</b> .....	11
<b>Ticket 3</b> .....	12

## 1. Instalación de la herramienta Catalyst.

Vamos a añadir dos líneas de texto al archivo hosts.

***sudo nano /etc/hosts***



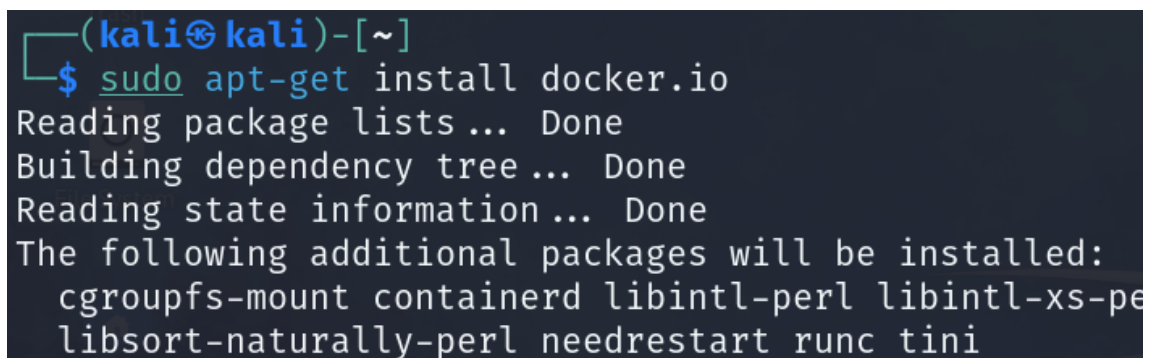
```
(kali㉿kali)-[~]  
$ sudo nano /etc/hosts
```

```
GNU nano 7.2 /etc/hosts *  
127.0.0.1 localhost  
127.0.1.1 kali  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters  
127.0.0.1 catalyst.localhost  
127.0.0.1 authelia.localhost
```

127.0.0.1 catalyst.localhost
127.0.0.1 authelia.localhost

Instalación de Docker.io.

***sudo apt-get install docker.io***



```
(kali㉿kali)-[~]  
$ sudo apt-get install docker.io  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  cgroupfs-mount containerd libintl-perl libintl-xs-perl  
  libsort-naturally-perl needrestart runc tini
```

Instalación de Curl.

***sudo apt-get install curl***

```
(kali㉿kali)-[~]  
$ sudo apt-get install curl  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:
```

Instalación Docker-compose.

***sudo apt-get install docker-compose***

```
(kali㉿kali)-[~]  
$ sudo apt-get install docker-compose  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  python3-compose python3-docker python3-dockerpty python3-texttable  
The following NEW packages will be installed:
```

Unzip ya lo teníamos instalado.

***sudo apt-get install unzip***

```
(kali㉿kali)-[~]  
$ sudo apt-get install unzip  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
unzip is already the newest version (6.0-28).  
unzip set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 1023 not upgraded.
```

Instalación openssl.

***sudo apt-get install openssl***

```
(kali㉿kali)-[~]  
$ sudo apt-get install openssl  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libssl3  
The following packages will be upgraded:  
  libssl3 openssl  
2 upgraded, 0 newly installed, 0 to remove and 1021 not upgraded.
```

Instalación de sed.

***sudo apt-get install sed***

```
(kali㉿kali)-[~]  
$ sudo apt-get install sed  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages will be upgraded:  
  sed  
1 upgraded, 0 newly installed, 0 to remove and 1020 not upgraded.
```

Ahora vamos a descargarnos el script de instalación.

***curl -sL https://raw.githubusercontent.com/SecurityBrewery/catalyst-setup/v0.10.3/install\_catalyst.sh -o install\_catalyst.sh***

```
(kali㉿kali)-[~]  
$ curl -sL https://raw.githubusercontent.com/SecurityBrewery/catalyst-setup/v0.10.3/install_catalyst.sh -o install_catalyst.sh  
(kali㉿kali)-[~]  
$ ls  
Desktop Documents Downloads install_catalyst.sh Music Pictures PrácticaPKIPAR Prueba Public Templates Videos
```





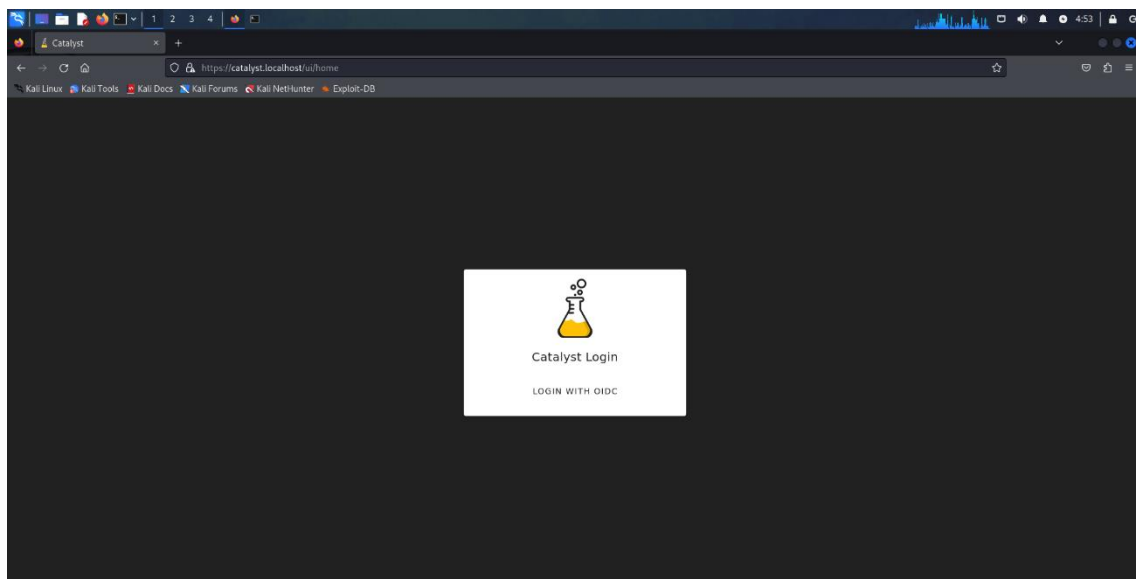
Ahora podemos observar como la instalación se hace correctamente

```
(kali@kali)-[~]
$ sudo bash install_catalyst.sh \
https://catalyst.localhost \
https://authelia.localhost \
/home/kali/example.crt /home/kali/example.key \
admin:admin:admin@example.com


Archive: catalyst_install.zip
b01486f9b6abef843bf64644bfdbca339d8821a4
replace catalyst-setup-0.10.3/.gitignore? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: catalyst-setup-0.10.3/.gitignore
replace catalyst-setup-0.10.3/authelia/configuration.tpl.yml? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: catalyst-setup-0.10.3/authelia/configuration.tpl.yml
replace catalyst-setup-0.10.3/docker-compose.tpl.yml? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: catalyst-setup-0.10.3/docker-compose.tpl.yml
replace catalyst-setup-0.10.3/install_catalyst.sh? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: catalyst-setup-0.10.3/install_catalyst.sh
replace catalyst-setup-0.10.3/nginx/nginx-ssl.tpl.conf? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: catalyst-setup-0.10.3/nginx/nginx-ssl.tpl.conf
replace catalyst-setup-0.10.3/nginx/nginx.tpl.conf? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: catalyst-setup-0.10.3/nginx/nginx.tpl.conf
replace catalyst-setup-0.10.3/renovate.json? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: catalyst-setup-0.10.3/renovate.json
writing RSA key
Pulling arangodb ... done
Pulling minio ... done
Pulling authelia ... done
Pulling catalyst ... done
Pulling nginx ... done
arangodb uses an image, skipping
minio uses an image, skipping
authelia uses an image, skipping
catalyst uses an image, skipping
nginx uses an image, skipping
Creating network "catalyst" with the default driver
Creating volume "catalyst-setup-0103_arangodb" with default driver
Creating volume "catalyst-setup-0103_minio" with default driver
Creating catalyst-setup-0103_arangodb_1 ... done
Creating catalyst-setup-0103_minio_1 ... done
```

Accediendo a Catalyst.

Una vez instalada podemos acceder a ella desde el navegador poniendo catalyst.localhost



Usuario y contraseña: admin admin



Sign in

Username \*

admin

Password \*

•••••


☐ Remember me

SIGN IN

[Reset password?](#)

Powered by Authelia

Aceptaremos





Hi admin


Consent Request

API

The above application is requesting the following permissions:

 Use OpenID to verify your identity

 Access your profile information

 Access your email addresses

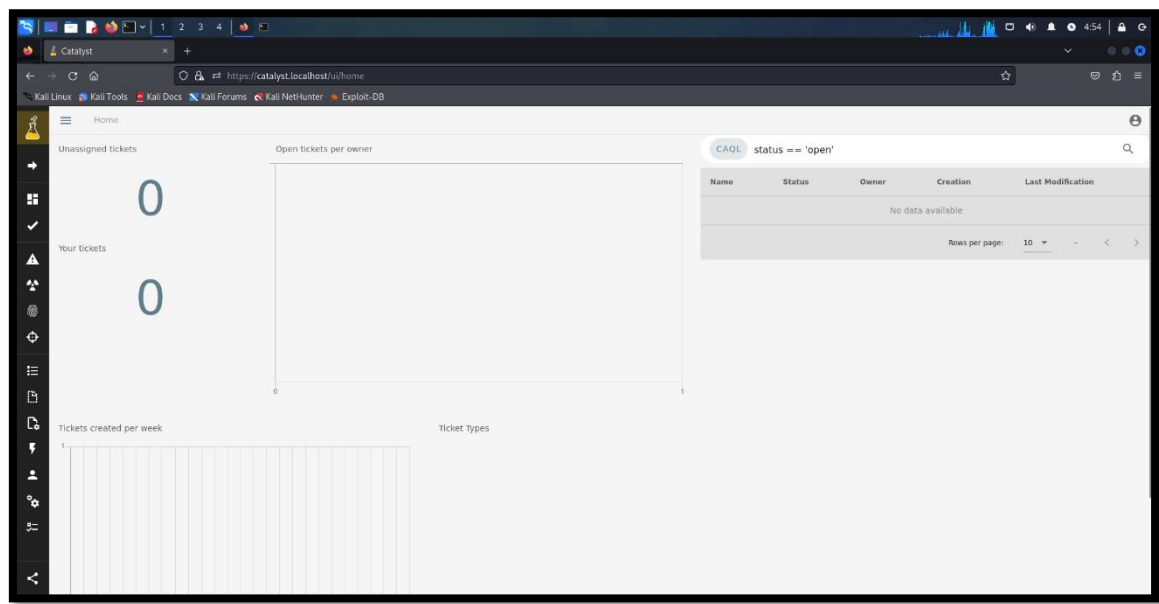
ACCEPT

DENY

Powered by Authelia



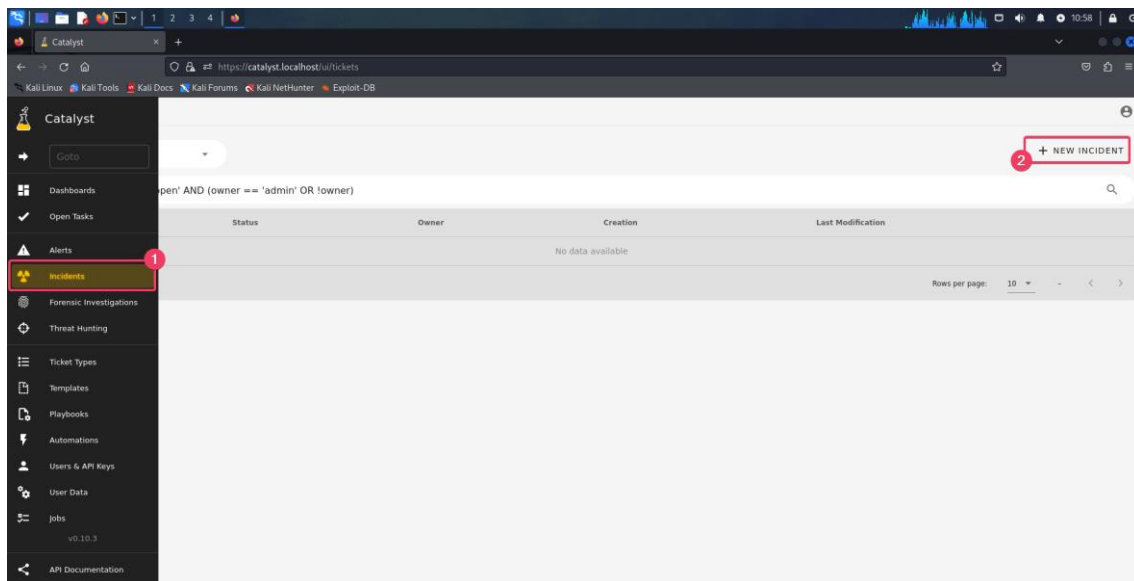
Y ya estaríamos dentro de Catalyst.



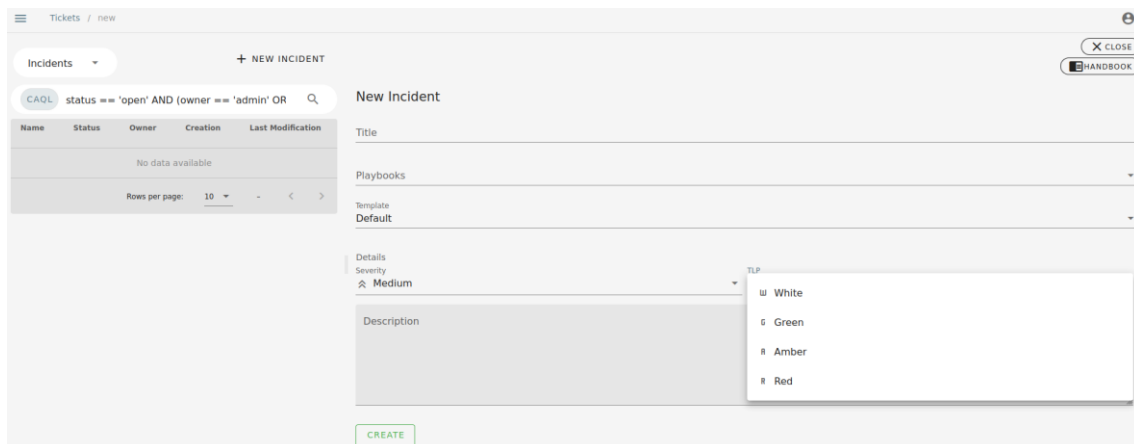
## 2. Una vez instalada usa la herramienta Catalyst y crea 3 tickets sobre incidentes que hayas catalogado en la actividad 3.1, prestando atención a la taxonomía del incidente descrito. Detalla todos los pasos.

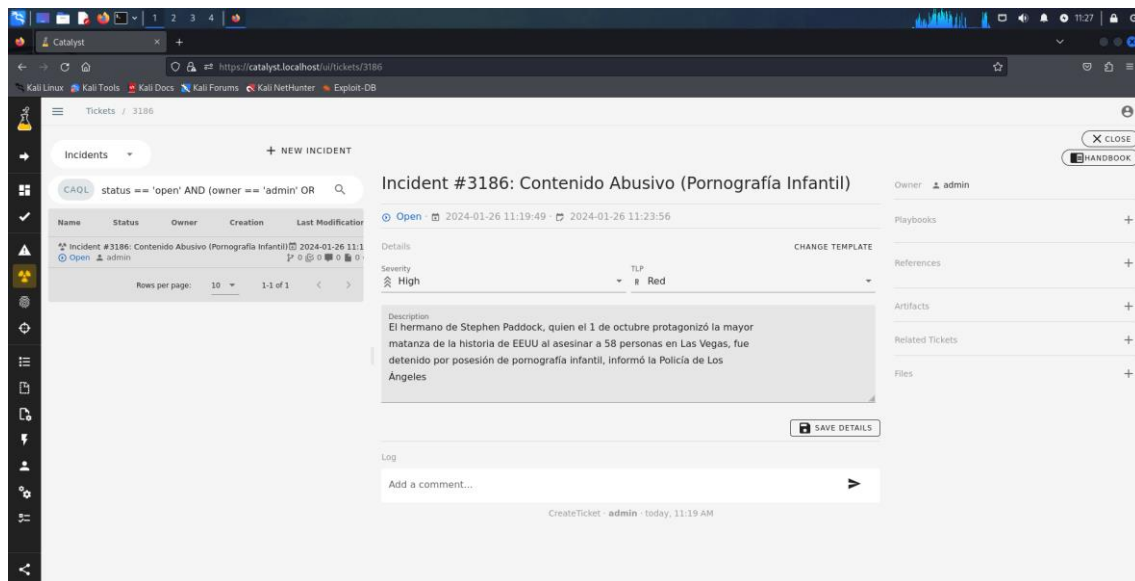
### Ticket 1

Incidents -> New Incident



Aquí estamos ya en la pestaña en la que se crean los incidentes. En ella hay que poner un título, una descripción, la severidad del incidente y el Traffic Light Protocol (White, Green, Amber or Red).



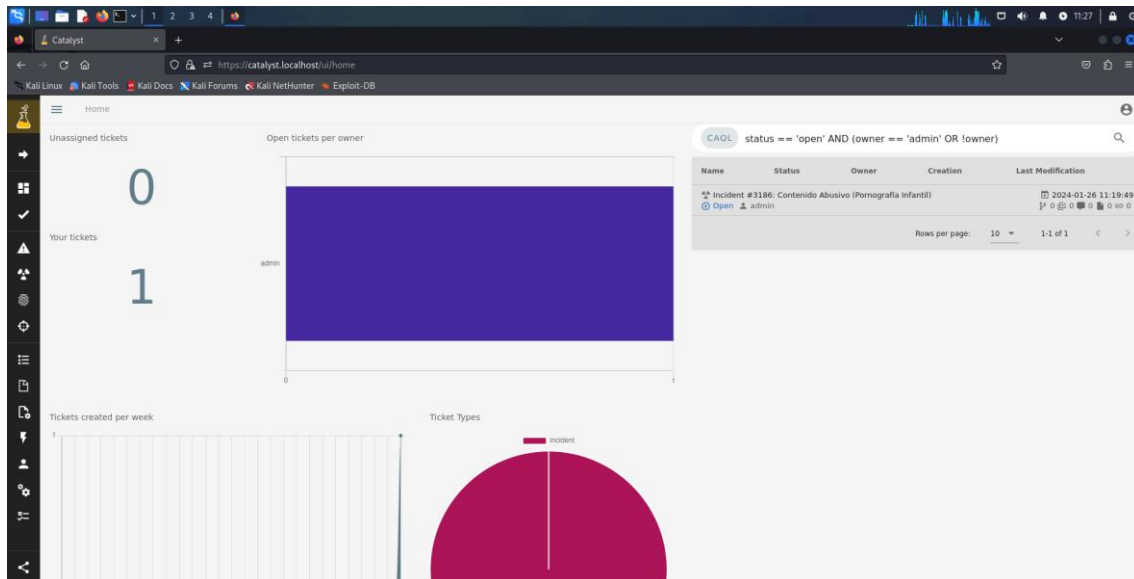


➤ **Severidad: High**

La asignación de la severidad "High" se basa en la gravedad extrema del contenido identificado, que incluye la presencia de pornografía infantil. Este material no solo es ilegal, sino que también presenta un riesgo inmediato y significativo para la seguridad y el bienestar de los menores involucrados. La seriedad del incidente demanda una respuesta urgente para eliminar cualquier amenaza potencial, proteger a los afectados y asegurar la aplicación rigurosa de medidas legales.

➤ **TLP: Red**

La designación "Red" de confidencialidad se justifica por la urgencia de mantener la máxima discreción debido a la gravedad del contenido. La información se comparte solo con autoridades altamente autorizadas para preservar la integridad de las investigaciones y proteger la identidad de los menores afectados. Esta combinación con la severidad "High" refleja la gravedad del incidente y la necesidad de una respuesta rápida y efectiva.



## Ticket 2

The screenshot shows the details of Incident #1887: Agència Catalana de Notícies (ACN) Intrusión (Compromiso del sistema). The incident is in 'Open' status, created on 2024-01-30 11:12:50, and last modified on 2024-01-30 11:12:50. The severity is 'Medium' and the TLP is 'Amber'. The description states: 'La Agència Catalana de Notícies (ACN) ha sofert en els últims dies un intent de ciberataque, segons ha informat el mateix mitjà. El atac, sin embargo, no ha tenido consecuencias sobre el sistema ni ha afectado a su servicio, ya que se pudo detectar a tiempo. Los sistemas de detección y vigilancia de la Agencia de Ciberseguridad identificaron el viernes pasado por la tarde la existencia de una'. The incident is owned by 'admin'.

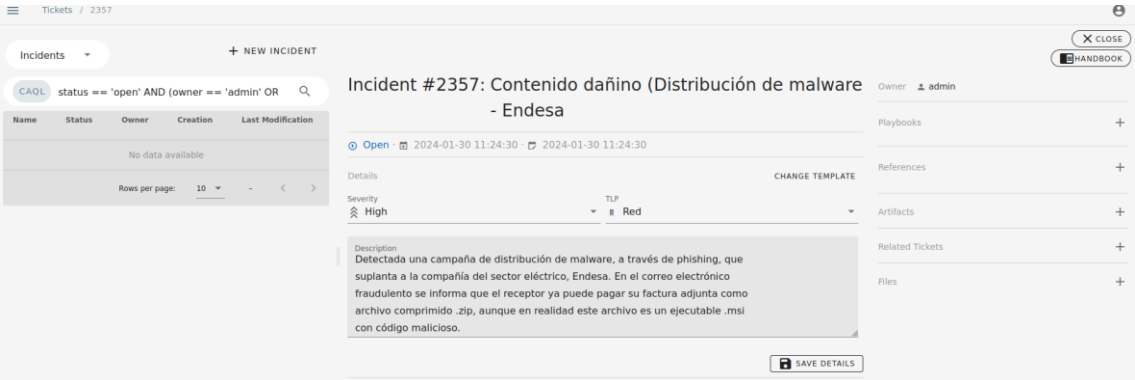
### ➤ Severidad: Medium

Aunque hubo un intento de intrusión, no se produjeron consecuencias significativas para el sistema ni se afectó el servicio. Aunque se activaron alertas y se tomaron medidas, la situación no alcanzó un nivel crítico, y la intervención temprana evitó daños mayores.

### ➤ TLP: Amber

La información sobre el intento de ciberataque debe ser compartida de manera restringida con aquellos que necesiten conocerla para tomar medidas de seguridad. Aunque el ataque no tuvo éxito y no afectó los servicios, la naturaleza de la intrusión ilegítima requiere cierta cautela en la divulgación.

Ticket 3

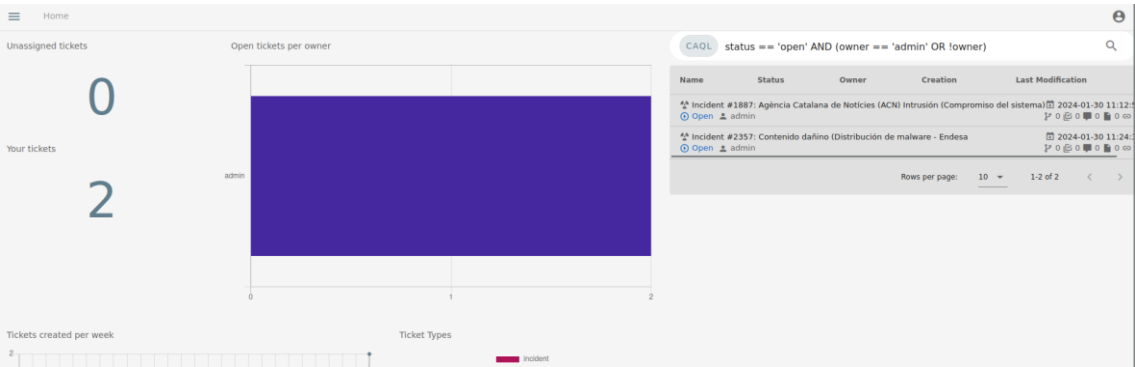


➤ Severidad: High

Se clasifica como "High" debido a la peligrosidad extrema de la situación. La campaña de distribución de malware mediante phishing, que suplanta a una entidad confiable como Endesa y afecta a infraestructuras críticas, representa una amenaza inminente y de alto riesgo para la seguridad de un gran número de usuarios.

➤ TLP: Red

La información sobre una campaña de distribución de malware que utiliza phishing para suplantar una compañía eléctrica y afecta a infraestructuras críticas y a un gran número de usuarios se clasifica como "Red". La gravedad y el impacto potencial son significativos, y la información debe ser compartida de manera confidencial y restringida a aquellos con necesidad y autorización.



Podemos ver sólo dos tickets creados, ya que el primero de ellos lo he creado en casa.