



---

# HERRAMIENTA FIR

---

PRÁCTICA 3.3

ERIC SERRANO MARÍN  
INCIDENTES DE CIBERSEGURIDAD

Contenido

1. Instalación, uso y configuración..... 2

    Ticket 1 ..... 4

    Ticket 2 ..... 4

2. Caso Práctico. .... 7

## 1. Instalación, uso y configuración.

- Instala la herramienta FIR (Fast Incident Response) haciendo uso de docker-compose.

Clonamos el repositorio de FIR en de github.

***git clone https://github.com/certsocietegenerale/FIR.git***

```
(kali㉿kali)-[~]  
$ git clone https://github.com/certsocietegenerale/FIR.git  
Cloning into 'FIR' ...  
remote: Enumerating objects: 3821, done.  
remote: Counting objects: 100% (1016/1016), done.  
remote: Compressing objects: 100% (207/207), done.  
remote: Total 3821 (delta 841), reused 833 (delta 808), pack-reused 2805  
Receiving objects: 100% (3821/3821), 2.18 MiB | 4.83 MiB/s, done.  
Resolving deltas: 100% (2127/2127), done.
```

Creamos la imagen con docker-compose.

***sudo docker-compose build***

```
(kali㉿kali)-[~/FIR/docker]  
$ sudo docker-compose build  
fir_db uses an image, skipping  
fir_redis uses an image, skipping  
fir_celery_worker uses an image, skipping  
fir_celery_beat uses an image, skipping  
fir_web uses an image, skipping  
Building fir  
Sending build context to Docker daemon 4.251MB
```

Aquí podemos observar como ha finalizado (14/14).

```
→ aa3c6e6a1e8a  
Step 14/14 : CMD ["runserver", "--settings", "fir.config.production", "0.0.0.0:8000"]  
→ Running in 9e7305c65a83  
Removing intermediate container 9e7305c65a83  
→ 8f6c28d0a976  
Successfully built 8f6c28d0a976  
Successfully tagged fir:latest
```

Procedemos a iniciar FIR.

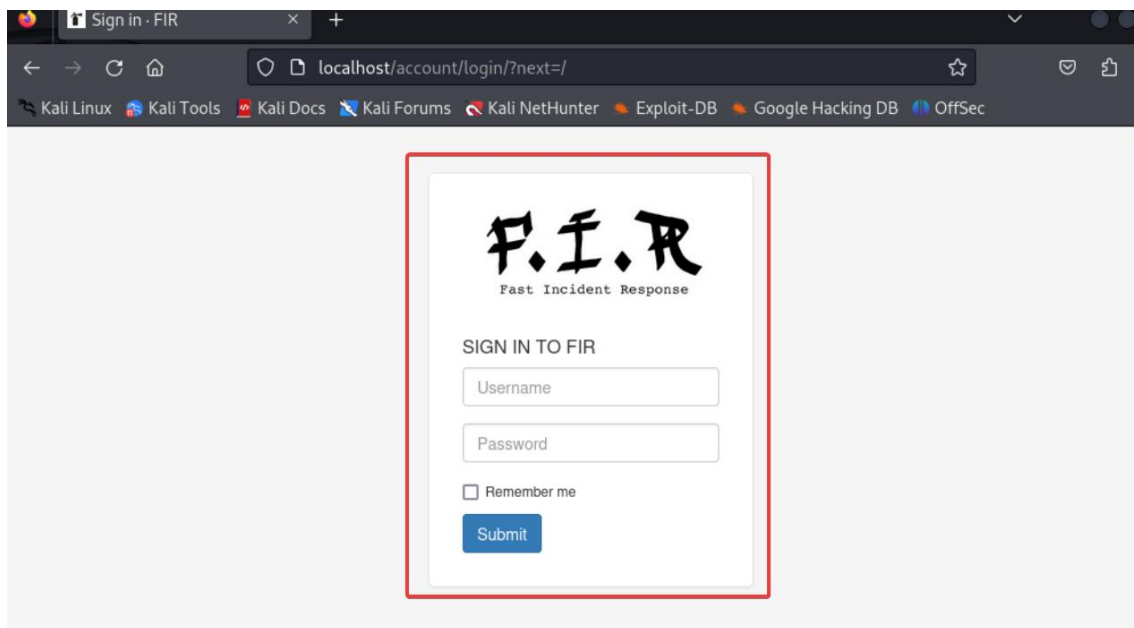
***sudo docker-compose up -d***

```
(kali㉿kali)-[~/FIR/docker]  
$ sudo docker-compose up -d  
Creating network "docker_backend.fir" with the default driver  
Creating volume "docker_static-content" with default driver  
Creating volume "docker_mariadb-data" with default driver  
Pulling fir_db (mariadb)...  
latest: Pulling from library/mariadb  
29202e855b20: Pull complete
```

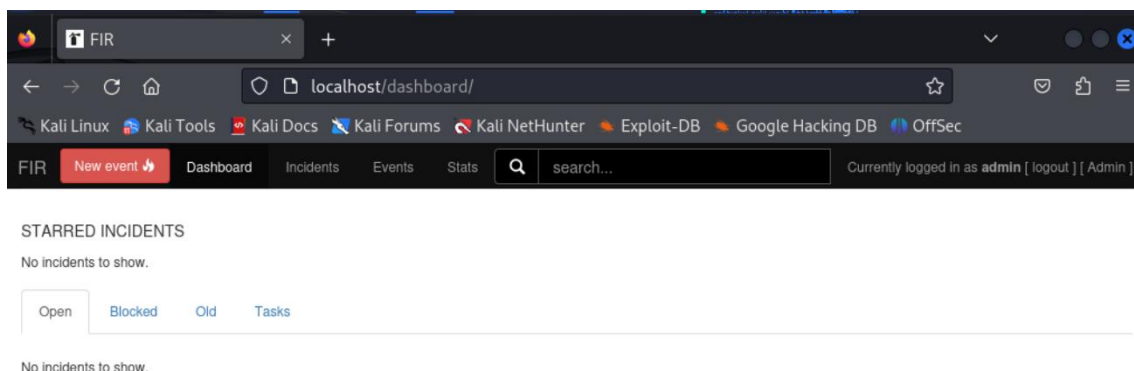
```
Status: Downloaded newer image for nginx:latest
Creating fir_redis ... done
Creating fir_db ... done
Creating fir ... done
Creating fir_web ... done
Creating fir_celery_beat ... done
Creating fir_celery_worker ... done
```

- Una vez lista, accede con las credenciales por defecto (admin/admin o dev/dev) y haz uso de la misma para crear 2 incidentes encontrados para la práctica 2.1 y que no hayas registrado en la práctica anterior.

Para acceder hemos puesto en el navegador: localhost.



Para entrar hemos usado admin admin.



Ticket 1

New event

Save

Summary

Subject

Ataque Disponibilidad Microsoft

Business Lines

Category

DoS

Status

Closed

Detection

SOC

Severity

2

Date / Time

2024-01-31 16:46

Confidentiality

C0

☐ Is an incident

Description

B I H<sub>1</sub> H<sub>2</sub> % <> | | | - | |

DoS a Microsoft, afectó a Outlook y One drive.

**Status:** Closed ya que el incidente ya se cerró.

**Confidentiality:** Green (C0), ya que la información puede ser compartida de manera más amplia para mejorar la conciencia y la preparación.

**Severity:** 2, debido a que, aunque las interrupciones afectaron gravemente a Microsoft y a sus servicios de correo electrónico y almacenamiento en la nube, no se mencionan consecuencias graves a nivel de seguridad.

Ticket 2

FIR New event Dashboard Incidents Events Stats search... Currently logged in as admin [ logout ] [ Admin ]

New event

Save

Summary

Subject

Fuga de datos - Vodafone

Business Lines

Category

Stolen data

Status

Closed

Detection

CERT

Severity

4

Date / Time

2024-01-31 17:17:04

Confidentiality

C3

☐ Is an incident

Description

B I H<sub>1</sub> H<sub>2</sub> % <> | | | - | |

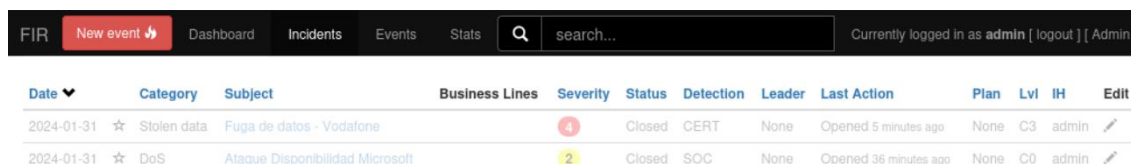
Vodafone ha dejado expuestos diferentes datos personales y bancarios de un número limitado de clientes de la operadora.

**Status:** Closed ya que el incidente ya se cerró.

Página 4 | 10

**Confidentiality:** Red (C3), necesidad de restringir la divulgación a un grupo selecto de personas con una necesidad directa de conocer la información y que estén autorizadas para abordar la situación

**Severity:** 4, debido a la naturaleza crítica de la incidencia de seguridad, que resultó en la fuga de datos personales y bancarios de clientes de Vodafone.

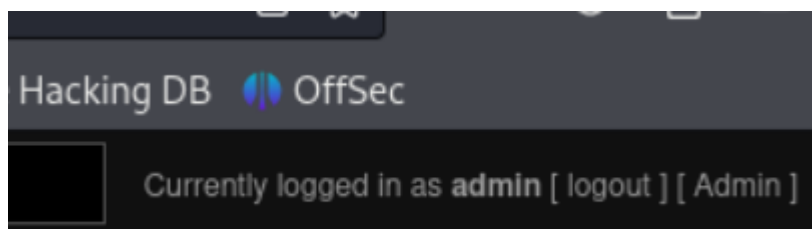


The screenshot shows the FIR dashboard with a table of incidents. The table has columns for Date, Category, Subject, Business Lines, Severity, Status, Detection, Leader, Last Action, Plan, Lvl, IH, and Edit. Two incidents are listed: one for 'Stolen data' (Severity 4) and one for 'DoS' (Severity 2).

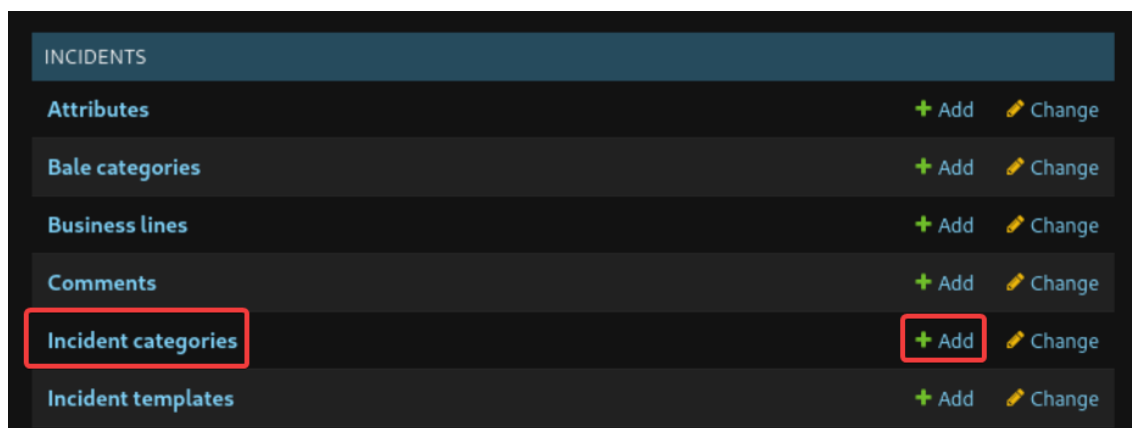
Date	Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2024-01-31	Stolen data	Fuga de datos - Vodafone		4	Closed	CERT	None	Opened 5 minutes ago	None	C3	admin	
2024-01-31	DoS	Ataque Disponibilidad Microsoft		2	Closed	SOC	None	Opened 36 minutes ago	None	C0	admin	

- Además, échale un vistazo a la configuración de la herramienta, para ver las distintas opciones que tiene la misma y crea una nueva categoría de incidente para usarlo en la Parte 2 de esta práctica.

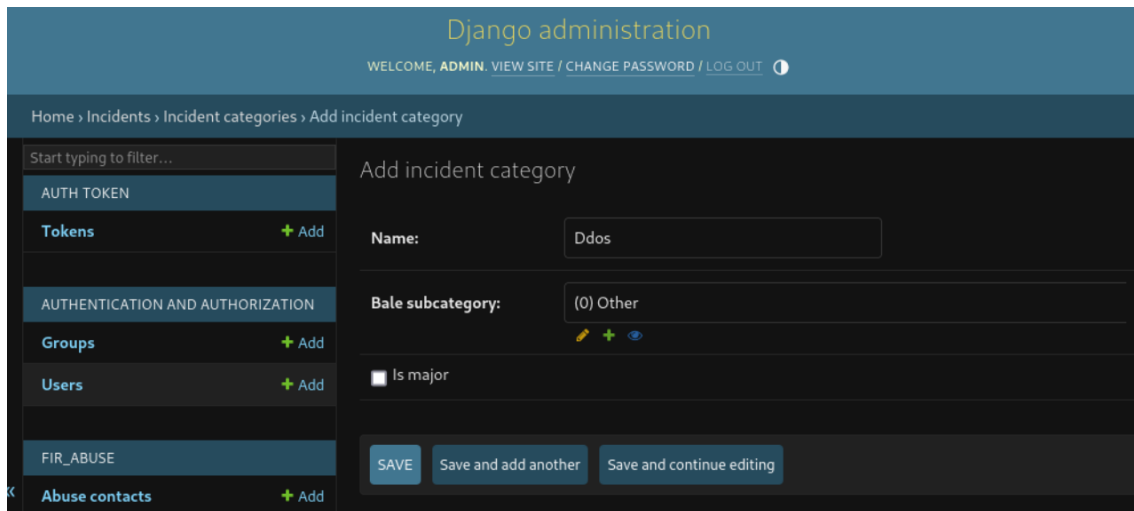
Para crear una nueva categoría de incidente primero haremos clic en Admin.



Buscaremos la parte de Incidents y haremos clic en Add en Incident categories.



Vamos a añadir Ddos.



Django administration

WELCOME, ADMIN. [VIEW SITE](#) / [CHANGE PASSWORD](#) / [LOG OUT](#)

Home » Incidents » Incident categories » Add incident category

Start typing to filter...

AUTH TOKEN

Tokens [+ Add](#)

AUTHENTICATION AND AUTHORIZATION

Groups [+ Add](#)

Users [+ Add](#)

FIR\_ABUSE

Abuse contacts [+ Add](#)

Add incident category

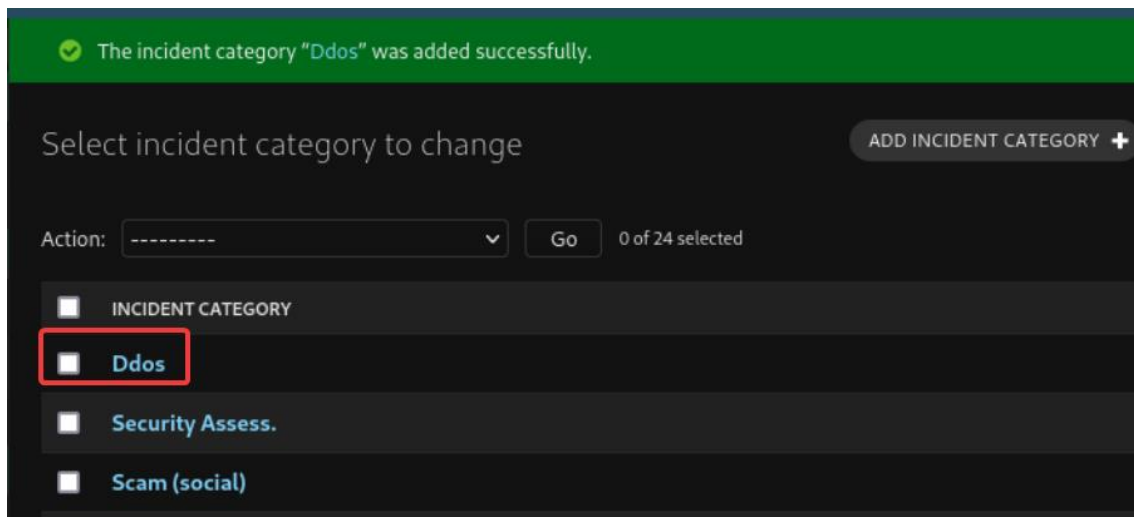
Name:

Bale subcategory:  [✎](#) [+](#) [👁](#)

☐ Is major

[SAVE](#) [Save and add another](#) [Save and continue editing](#)

Como podemos ver la nueva categoría de incidente se ha creado correctamente.



✓ The incident category "Ddos" was added successfully.

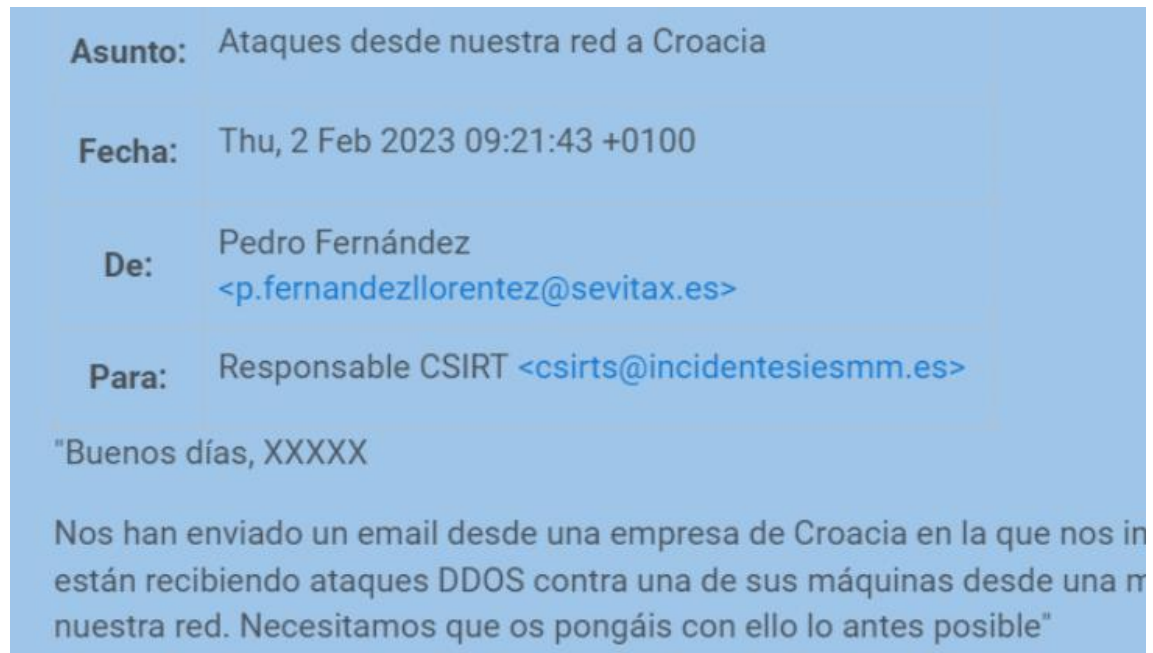
Select incident category to change [ADD INCIDENT CATEGORY +](#)

Action:  [Go](#) 0 of 24 selected

<input type="checkbox"/>	INCIDENT CATEGORY	
<input type="checkbox"/>	Ddos	
<input type="checkbox"/>	Security Assess.	
<input type="checkbox"/>	Scam (social)	

## 2. Caso Práctico.

Trabajas en CSIRT de una empresa y te llega la siguiente secuencia de correos



En ese momento registras en FIR el evento y le asignas la tarea a uno de los componentes del equipo para que lo investigue.

Recibes el siguiente email del técnico asignado:



Asunto:	Ataque Amplificación DNS en Sevitax
Fecha:	Thu, 2 Feb 2023 12:03:33 +0100
De:	Manuel CSIRT <manu.csirt@incidenteslesmm.es>
Para:	Responsable CSIRT <csirts@incidenteslesmm.es>

"Respecto al tema del ataque que estamos estudiando te pongo en situación:

Por lo que nos indican y hemos comprobado, desde Croacia están recibiendo ataques DDOS contra una de sus máquinas desde una máquina de la red (rango público) de Sevitax.

La situación que observamos cuadra con un tipo de ataque "Amplificación DNS", se hacen peticiones a servidores DNS abiertos a internet (como es el caso) con la ip de origen falseada (usando la del objetivo del ataque), esto provoca que los servidores DNS implicados en el ataque envíen respuestas de forma masiva a la ip atacada (la que va enmascarada en la petición al DNS) por lo tanto el ataque no es directamente al DNS de SEvitax aunque este se vea afectado, sino que lo están usándolo como parte de una especie de botnet (no es exactamente lo mismo ya que no hay ningún tipo de malware a nivel de servidor).

Por lo que he estado viendo para que un DNS sea vulnerable a este tipo de ataques es necesario que use recursividad y esta permita peticiones cualquier servidor, y este es exactamente el caso.

Configuración de los DNS, cualquiera puede usar recursividad:

```
allow-recursion { 0.0.0.0/0; };
```

Por lo que para solventar el problema vamos a restringir este parámetro a sólo a las redes/IPs que necesitan hacer uso de recursión, en este momento estamos trabajando en identificar esas redes/IPs y a lo largo del día de hoy esperamos tener el problema corregido.

Un saludo.

Manuel"

Modifica el evento registrado en función de los nuevos datos que te aporta el último email.

La categoría que crees debe reflejar lo que pasa realmente con este incidente. Justifica por qué has decidido crear esa categoría.

Haz capturas de los pasos y explica todo el proceso.

Primero he abierto un incidente con la poca información que tenía, lo he dejado abierto, dándole Severity de 4, ya que dice que es urgente y Confidentiality C2.

FIR

New event

Dashboard

Incidents

Events

Stats

search...

Currently logged in as admin [logout] [Admin]

New event

Save

Summary

Incident details

Subject

Business Lines

Actor

Plan

je desde nuestra red a Croacia

-----

-----

☐ Major incident

Category

Status

Detection

Severity

Ddos

Open

CERT

4

Date / Time

Confidentiality

2024-02-01 17:02:41

C2

☒ Is an incident

Description

B I H<sub>v</sub> H<sub>1</sub> % </>

Una empresa de Croacia está recibiendo ataques DDOS contra una de sus máquinas desde nuestra red

Incident Leader

None

Plan

None

Severity

4

Category

Ddos

Status

Open

Detection

CERT

B/L

## Incident / Ddos / Ataque desde nuestra red a Croacia

Opened on Feb. 1, 2024, 5:02 p.m. by admin

DESCRIPTION

Una empresa de Croacia está recibiendo ataques DDOS contra una de sus máquinas desde nuestra red

Comments (1)

Threat Intel

		Comment	Action
2024-02-01 17:02	admin	Incident opened	Opened

Después de haber recibido el segundo correo vamos a editar este incidente que hemos creado.

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

FIR

New event

Dashboard

Incidents

Events

Stats

search...

Currently logged in as admin [logout] [Admin]

Date	Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Conf	Leader	Action
2024-02-01	★ Ddos	Ataque desde nuestra red a Croacia		4	Open	CERT	None	Opened 8 minutes ago	None	C2	admin	
2024-01-31	★ Stolen data	Fuga de datos - Vodafone		4	Closed	CERT	None	Opened a day ago	None	C3	admin	
2024-01-31	★ DoS	Ataque Disponibilidad Microsoft		2	Closed	SOC	None	Opened a day ago	None	C0	admin	

Ahora sabemos más específicamente que tipo de ataque es, así que vamos a crearlo, ya que no lo tenemos para seleccionarlo en el programa.



Aquí podemos observar como ya está nuestro incidente actualizado.

FIR

New event

Dashboard

Incidents

Events

Stats

search...

Currently logged in as admin [ logout ] [ Admin ]

Incident Leader	None	Plan	None	Severity	4	Category	DNS amplification DDoS attack	Status	Open	Detection	CERT	B/L
-----------------	------	------	------	----------	---	----------	-------------------------------	--------	------	-----------	------	-----

Incident / DNS amplification DDoS attack / Ataque desde nuestra red a Croacia

Opened on Feb. 1, 2024, 5:02 p.m. by admin

DESCRIPTION

Hemos comprobado desde Croacia que se están recibiendo ataques DDoS contra una de sus máquinas Sercitax. El tipo de ataque cuadra con Amplificación DNS. Para corregir este problema hay que restringir el parámetro allow-recursion [0.0.0.0/0]. A lo largo del día esperamos tener el problema corregido.

Comments (1)

Artifacts (2)

Threat Intel

		Comment	Action
2024-02-01 17:02	admin	Incident opened	Opened