

## ***DFIR: Una introducción***



### **Tarea 1: Introducción**

#### **Objetivos de aprendizaje**

Las brechas e incidentes de seguridad ocurren a pesar de que los equipos de seguridad se esfuerzan al máximo por evitarlos en todo el mundo. La estrategia prudente en este escenario es prepararse para el momento en que ocurra un incidente para evitar ser tomados por sorpresa. Por ello, la Investigación Forense Digital y la Respuesta a Incidentes ( DFIR ) se han convertido en una materia esencial en la Seguridad Defensiva. En esta sesión, abordaremos algunos conceptos básicos de DFIR y presentaremos salas que amplían nuestro conocimiento sobre DFIR . La sesión abordará los siguientes temas:

- Introducción del DFIR
- Algunos conceptos básicos utilizados en el campo DFIR
- Los procesos de respuesta a incidentes utilizados en la industria
- Algunas de las herramientas utilizadas para DFIR

P: Lea los objetivos de aprendizaje

R: No se necesita respuesta

### **Tarea 2: La necesidad del DFIR**

P1: ¿Qué significa DFIR?

R1: Digital Forensics and Incident Response

P2: El DFIR requiere experiencia en dos campos. Uno de ellos es la informática forense. ¿Cuál es el otro?

R2: Incident Response

### Tarea 3: Conceptos básicos del DFIR

P1: Entre la RAM y el disco duro, ¿qué almacenamiento es más volátil?

R1: RAM

P2: Completa el ejercicio de creación de una línea de tiempo en el sitio estático adjunto. ¿Qué bandera aparece al completarlo?

**Instructions**

We have observed a malicious alert on our SIEM dashboard. It seems like someone was downloading a malicious package. Click on the alert below to add it to your timeline spreadsheet.

https://siem.internal

Countries

UK

US

Brazil

China

Russia

N. Korea

100

50

0

40%

30%

30%

Operations: Information

1/3

Alert Log

Date

Message

May 24th 2022 12:37:22

Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked.

Attack Timeline.xlsx

1

A

B

C

Time

Description

Source

**Instructions**

Since we identified an IP address in the alert, we filtered all the traffic related to that IP address in the SIEM dashboard. We find the malicious IP address connected through an open SSH port in these filtered results. Click to add this result to our spreadsheet. Drag the events in the spreadsheet to bring them in ascending order of time.

https://siem.internal

Alert Log (Filter IP: 202.22.241.34)

Date

Message

May 24th 2022 09:30:20

Incoming SSH Connection from 202.22.241.34 to 192.168.1.150 on port 22. The connection was allowed.

May 24th 2022 12:37:22

Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked

Attack Timeline.xlsx

1

A

B

C

Time

Description

Source

2

May 24th 2022 12:37:22

Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked.

SIEM

## Ordenamos los Timelines

**Instructions**

Now, we check the Syslog for the compromised host to see what activity was performed by the attacker that can be of help. Click on the 'successful login attempt' event to add it to the spreadsheet.

syslog

Date/Time	Type	Host	Message
24 May 2022 09:25:35	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:26:30	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:27:25	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:28:32	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:29:20	Failed Login	192.168.1.150	Failed remote login attempt observed on Destination IP 192.168.1.150 from Source IP 202.22.241.34
24 May 2022 09:30:22	Login Successful	192.168.1.150	User John Doe successfully logged into 192.168.1.150 remotely, from IP address 202.22.241.34

Attack Timeline.xlsx

A	B	C
Time	Description	Source
May 24th 2022 12:37:22	Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked.	SIEM
May 24th 2022 09:30:20	Incoming SSH Connection from 202.22.241.34 to 192.168.1.150 on port 22. The connection was allowed.	SIEM

## Ordenamos los Timelines

**Instructions**

We checked the Syslog to find other interesting artifacts from the logs.

syslog

Date/Time	Type	Host	Message
24 May 2022 11:55:45	Application Critical	192.168.1.150	John Doe executed file name 'malicious-file'
24 May 2022 12:37:22	Application Critical	192.168.1.150	The process 'malicious-file' tried to connect to IP address 202.22.241.34

Attack Timeline.xlsx

A	B	C
Time	Description	Source
May 24th 2022 12:37:22	Source IP 192.168.1.150 tried to download Cobalt Strike from 202.22.241.34. The connection was blocked.	SIEM
May 24th 2022 09:30:20	Incoming SSH Connection from 202.22.241.34 to 192.168.1.150 on port 22. The connection was allowed.	SIEM
24 May 2022 09:30:22	User John Doe successfully logged into 192.168.1.150 remotely, from IP address 202.22.241.34	SYSLOG

### Challenge Complete

Congrats! You successfully created an incident timeline

**THM{DFIR\_REPORT\_DONE}**

R2: THM{DFIR\_REPORT\_DONE}

#### **Tarea 4:** Herramientas DFIR

P: Consulta las salas relacionadas con las diferentes herramientas mencionadas aquí.

R: No se necesita respuesta

#### **Tarea 5:** El proceso de respuesta a incidentes

P1: ¿En qué etapa del proceso de IR se restablecen los servicios interrumpidos a como estaban antes del incidente?

R1: Recovery

P2: ¿En qué etapa del proceso de IR se expulsa la amenaza de la red después de realizar el análisis forense?

R2: Eradication

P3: ¿Cuál es el equivalente NIST del paso denominado “Lecciones aprendidas” en el proceso SANS?

R3: Post-incident Activity

#### **Tarea 6:** Conclusión

Eso fue todo por esta sala. Repasemos lo que aprendimos aquí.

- Aprendimos qué es DFIR y dónde se utiliza.
- Aprendimos por qué necesitamos realizar DFIR .
- Aprendimos conceptos básicos como la cadena de custodia , la preservación de la evidencia y el orden de volatilidad.
- Aprendimos sobre algunas de las herramientas utilizadas en la industria como EZ tools, KAPE , Autopsy, etc.
- El proceso PICERL para respuesta a incidentes

Ahora podemos pasar a las siguientes salas de este módulo para aprender más sobre DFIR . Cuéntanos qué te pareció esta sala en nuestro canal de Discord o en nuestra cuenta de Twitter . Nos vemos.

P: Únete a la discusión en nuestros canales sociales.

R: No se necesita respuesta

---

 **LinkedIn:** <https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/>

 **GitHub:** <https://github.com/MaateoSuar>

