TAREA 05

DETECCIÓN Y DOCUMENTACIÓN DE INCIDENTES DE CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

Blue Team (Let's defend)
El equipo azul (blue team) en ciberseguridad se refiere a un equipo dedicado a la defensa de una organización contra posibles amenazas de seguridad cibernética. El blue team lleva a cabo actividades como la detección y respuesta a incidentes, la evaluación continua de la seguridad y la implementación de medidas de seguridad proactivas para prevenir futuros ataques. El objetivo del blue team es proteger los sistemas y datos de la organización, manteniendo un alto nivel de seguridad y disponibilidad.

La web "https://letsdefend.io/" es una plataforma que ofrece soluciones y servicios en el ámbito de la ciberseguridad, como la formación y el entrenamiento en habilidades técnicas para la defensa cibernética, así como pruebas de penetración y evaluaciones de seguridad para empresas y organizaciones.

Introducción: Descripción del caso práctico.
"Eres parte del equipo de ciberseguridad de la sede ministerial de Justicia en Andalucía. Todo parece estar funcionando de manera normal hasta que un día recibes una llamada urgente del responsable del departamento de TI. Algo va mal en los sistemas y hay un posible ciberataque en curso.
Rápidamente te diriges a la oficina y comienzas a investigar. Descubres a través del SIEM que existe un patrón de actividad sospechosa que indica un posible ataque. Inmediatamente, comienzas a investigar con tu equipo y a profundizar en los detalles del incidente. Descubrís que se ha producido una brecha en la seguridad y que los datos confidenciales están en riesgo…"

La plataforma "https://letsdefend.io" tiene una sección de simulación de productos SIEM como IBM Qradar, ArcSight ESM, etc. Como analista de SOC, una de tus tareas principales puede ser monitorear y analizar las alertas mostradas en un SIEM.
Elige una de las actividades sospechosas de la sección "Practice - Monitoring", simulando que puede ser uno de los posibles ataques recibidos en el anterior relato ficticio. Para este "evento" elegido se debe realizar un análisis (write-up) con el resultado de la investigación realizada.
Además, se debe indicar las distintas comunicaciones que deberían realizarse en caso de confirmarse un incidente de ciberseguridad en los sistemas.

Apartado 1: Write-up de un incidente.
Elige un incidente con categoría "High" o "Critical" del "SIEM" de "Letsfend.io" y redacta un documento con la investigación realizada y con los resultados obtenidos.
He seleccionado la siguiente incidencia:
High Web Attack, EventID: 263 - [SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]]

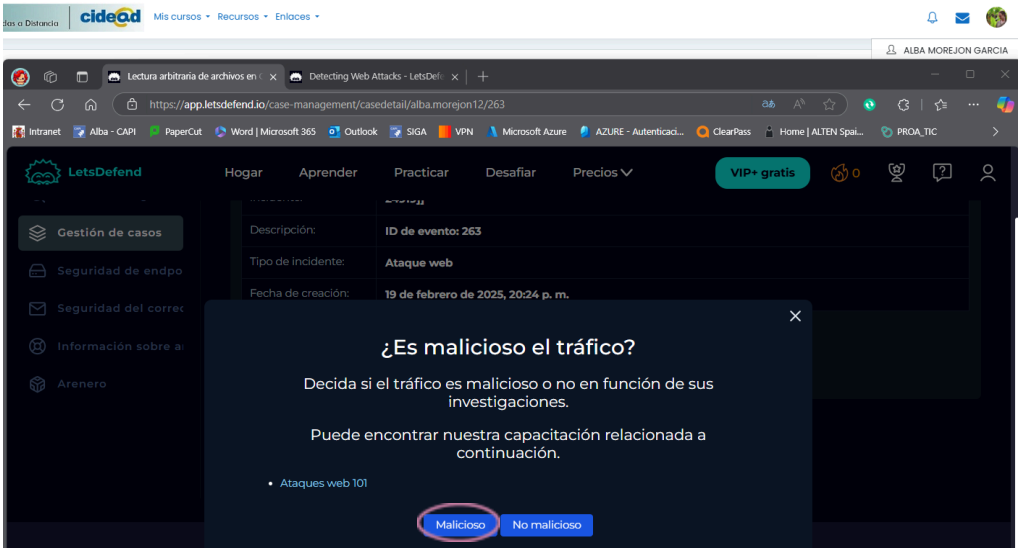
Write-Up: explicación del proceso de investigación que llevas a cabo para determinar si la alerta se trata de un falso positivo o si realmente es un incidente.
El incidente elegido es un ataque web en el que alguien intentó acceder a un archivo importante llamado /etc/passwd, que contiene información sobre los usuarios del sistema. El atacante logró navegar a través de las carpetas del sistema con alguna herramienta, y el sistema no bloqueó el intento, por lo que pudo acceder a dicho archivo.

Al investigar, se identificó un comportamiento sospechoso en el tráfico. Se reconoció un intento de acceso a un archivo sensible (/etc/passwd) desde la dirección IP 203.160.68.12 con un navegador Firefox utilizando un sistema operativo MacOS, lo que sugiere que el ataque vino desde fuera de la red de la empresa. El host afectado lleva el nombre de CP-Sark-Gateway-01 y la dirección IP 172.16.20.146. La alerta se disparó debido a un patrón de explotación de una vulnerabilidad conocida (CVE-2024-24919), que permite a los atacantes acceder a archivos del sistema, debido a un problema de seguridad en el sistema.

El ataque fue exitoso y no se trata de un falso positivo, esto significa que un atacante pudo acceder al archivo sensible y no fue un error del sistema.

A continuación, realizaremos el playbook que nos ofrece la página “letsdefend.io” sobre este incidente, en el que seguiremos una guía o modo de proceder para un tipo de ataque genérico, donde responderemos a diferentes preguntas para recopilar los datos importantes.

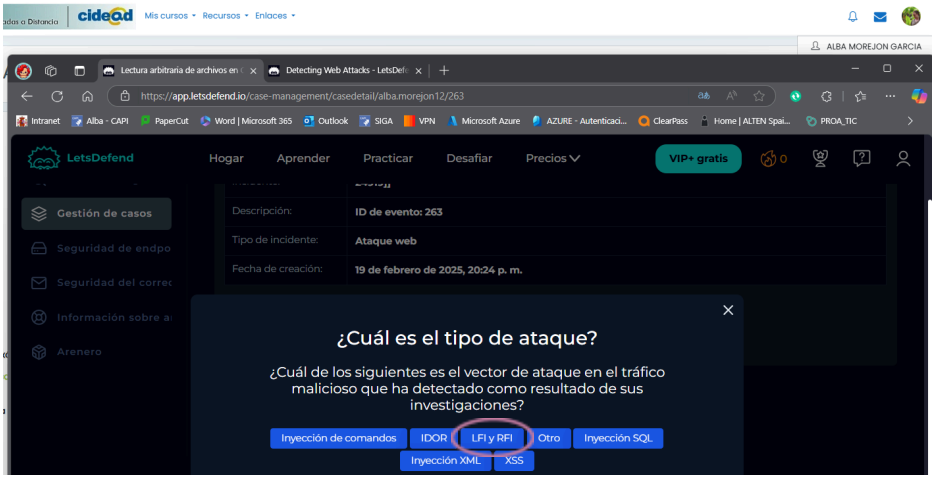
1- ¿Es malicioso el tráfico? Decida si el tráfico es malicioso o no en función de sus investigaciones.
La solicitud HTTP contiene un intento de acceder al archivo /etc/password. Coincide con un patrón característico de un intento de explotación de la vulnerabilidad (Zero Day) CVE-2024-24919 para la lectura de archivos restringidos. La solicitud HTTP POST seguramente contenga información maliciosa para hackear el acceso, junto con la dirección IP externa indican que es un comportamiento sospechoso.
Respuesta: Malicioso



2- ¿Cuál es el tipo de ataque? ¿Cuál de los siguientes es el vector de ataque en el tráfico malicioso que ha detectado como resultado de sus investigaciones?

LFI (Local file Inclusion), permite a un atacante incluir archivos en un servidor web manipulando parámetros en las solicitudes HTTP. El tipo de ataque es una Lectura Arbitraria de Archivos (LFI) , el vector de ataque en el tráfico detectado coincide con el descrito, el atacante accedió a la carpeta sensible utilizando una técnica de transversal de archivos.

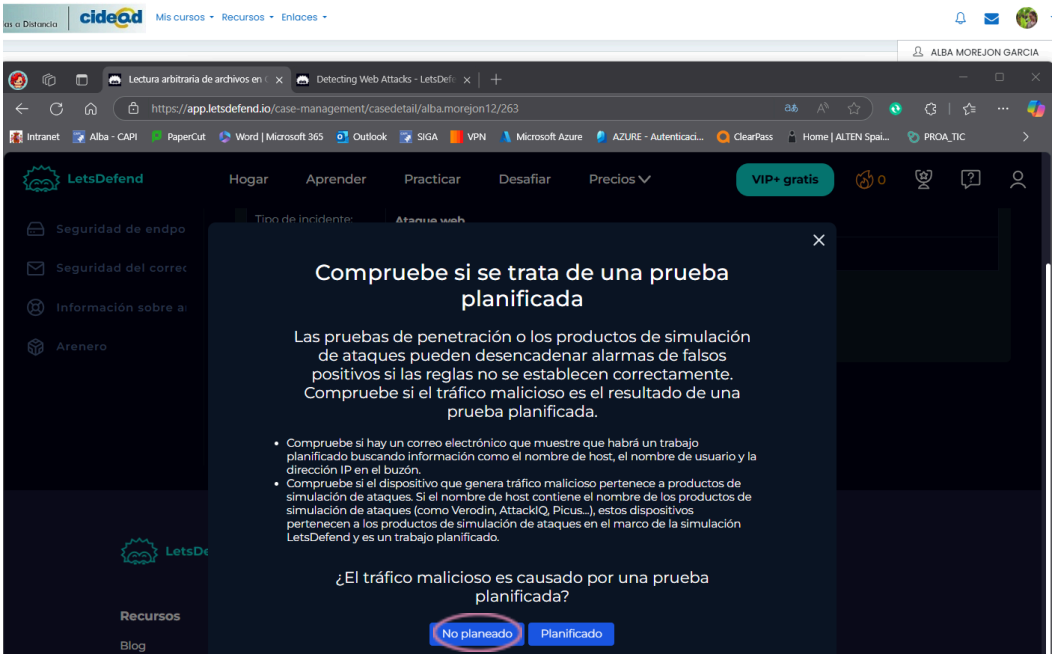
Respuesta: LFI y RFI



3- Compruebe si se trata de una prueba planificada. ¿El tráfico malicioso es causado por una prueba planificada?

No se encontró ningún correo electrónico que indique un trabajo planificado relacionado con la dirección 203.160.68.12 o el host CP-Sark-Gateway-01, que tampoco coincide con ningún nombre que coincida con los productos de simulación de ataques.

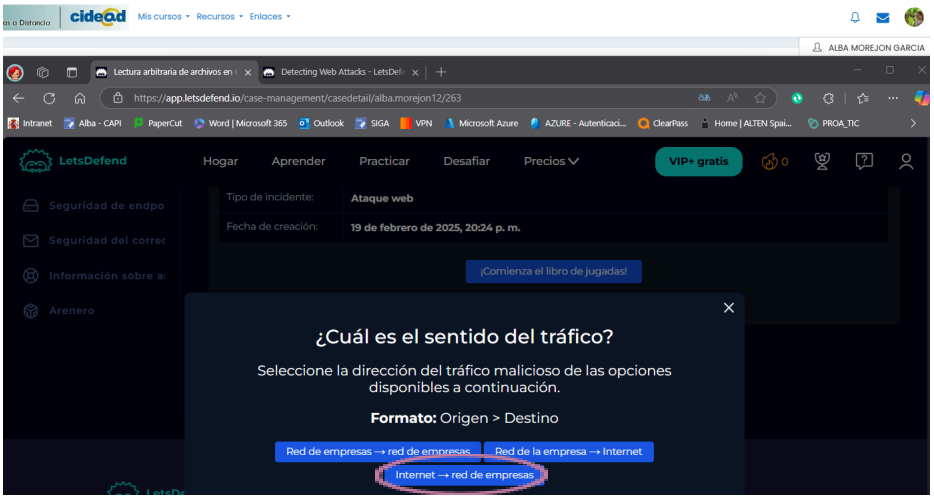
Respuesta: No planificado



4- ¿Cuál es el sentido del tráfico? Seleccione la dirección del tráfico malicioso de las opciones disponibles a continuación. Formato: Origen > Destino

El tráfico se origina desde una dirección de origen externo a la red (Internet) y la dirección de destino pertenece a la red interna de la empresa.

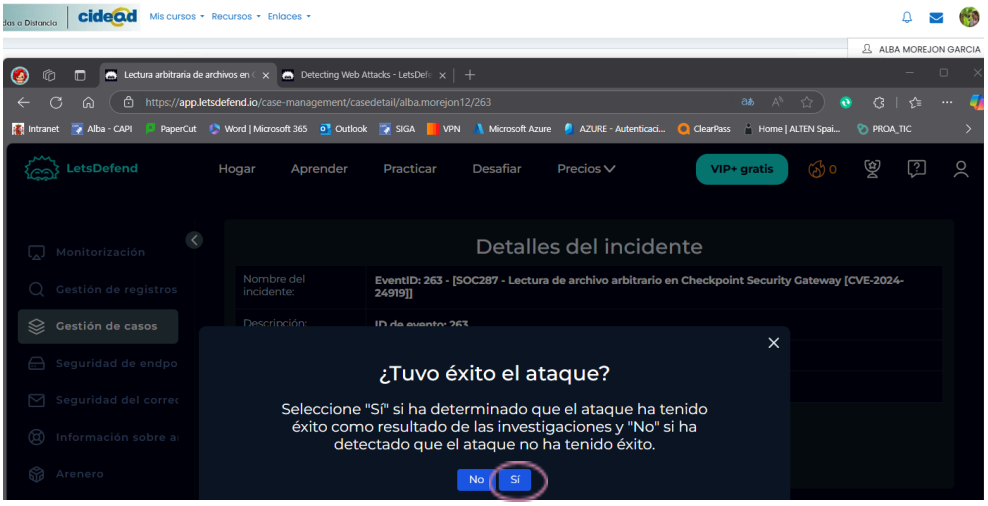
Respuesta: Internet -> Red de empresas



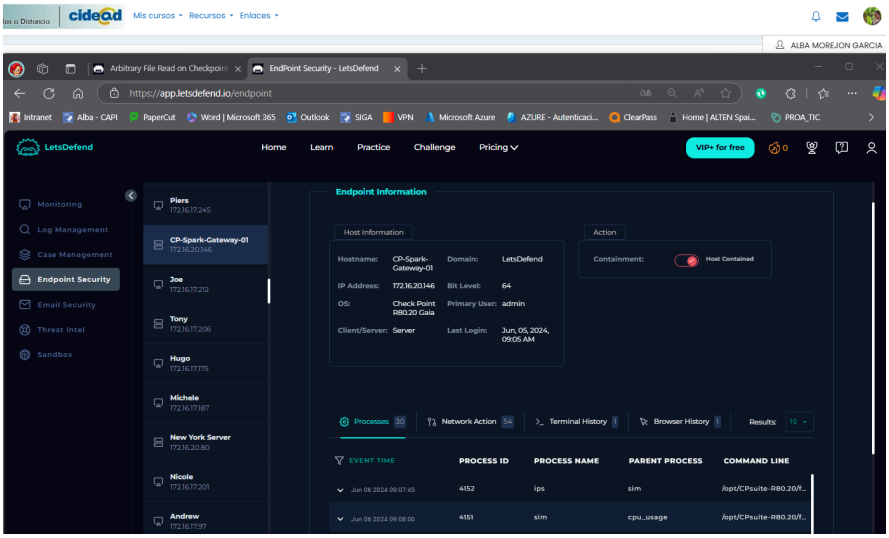
5- ¿Tuvo éxito el ataque? Seleccione "Sí" si ha determinado que el ataque ha tenido éxito como resultado de las investigaciones y "No" si ha detectado que el ataque no ha tenido éxito.

La investigación reveló que el atacante logró acceder al archivo /etc/passwd, lo que indica que la vulnerabilidad fue explotada con éxito. Se hizo un acceso no autorizado a información sensible.

Respuesta: Sí

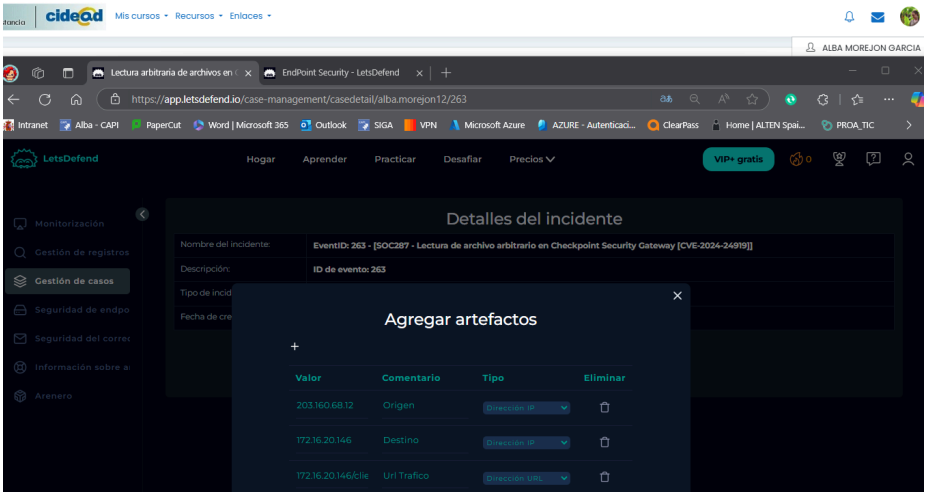


En el apartado de “Endpoint Security” encontramos el nombre del host involucrado en este incidente: “CP-Sark-Gateway-01” y siguiendo las indicaciones activamos el “Host contained”.
En esta página podemos visualizar los procesos y las acciones en la red.



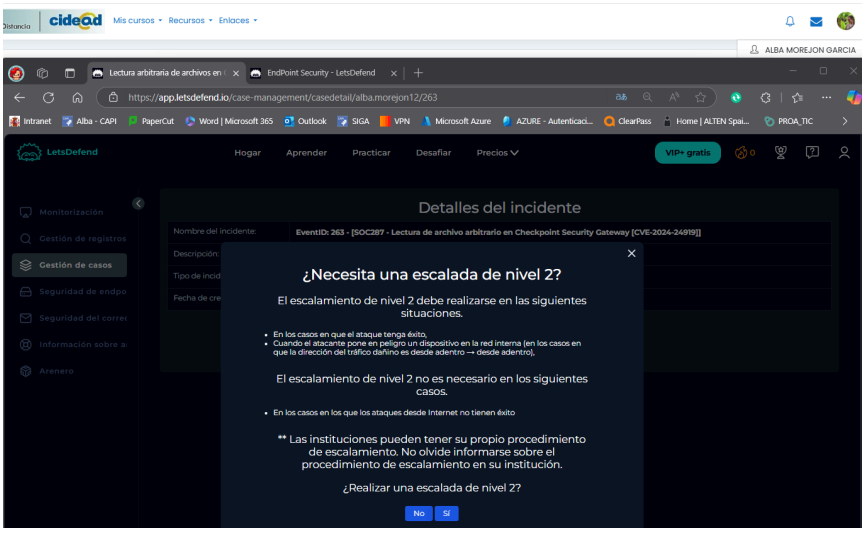
6- Agregar artefactos

Continuamos con el análisis y añadimos los artefactos identificados, la dirección IP origen, la dirección IP destino y la URL de solicitud.



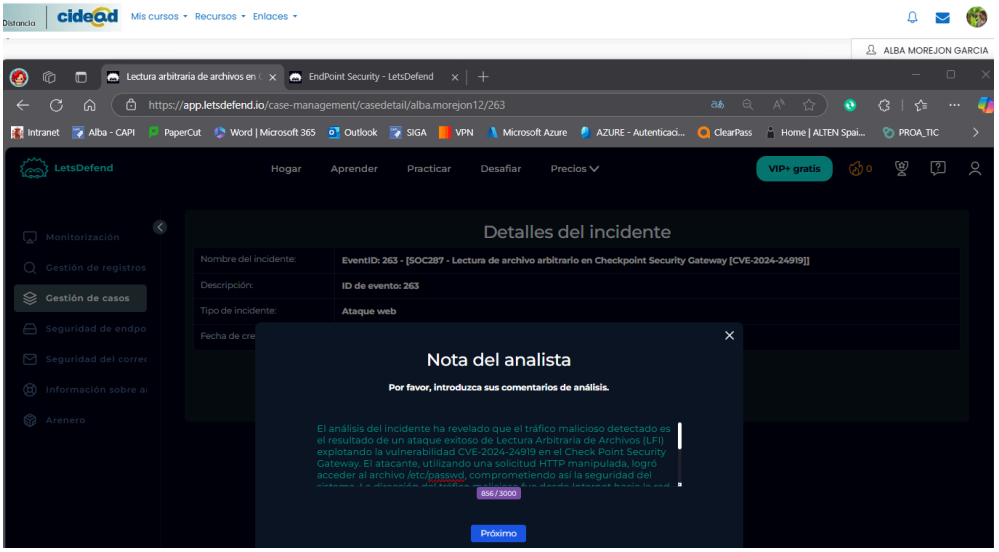
7- ¿Necesita una escalada de nivel 2?

El ataque tuvo éxito y un dispositivo de la red interna se ha visto afectado.
Respuesta: Sí



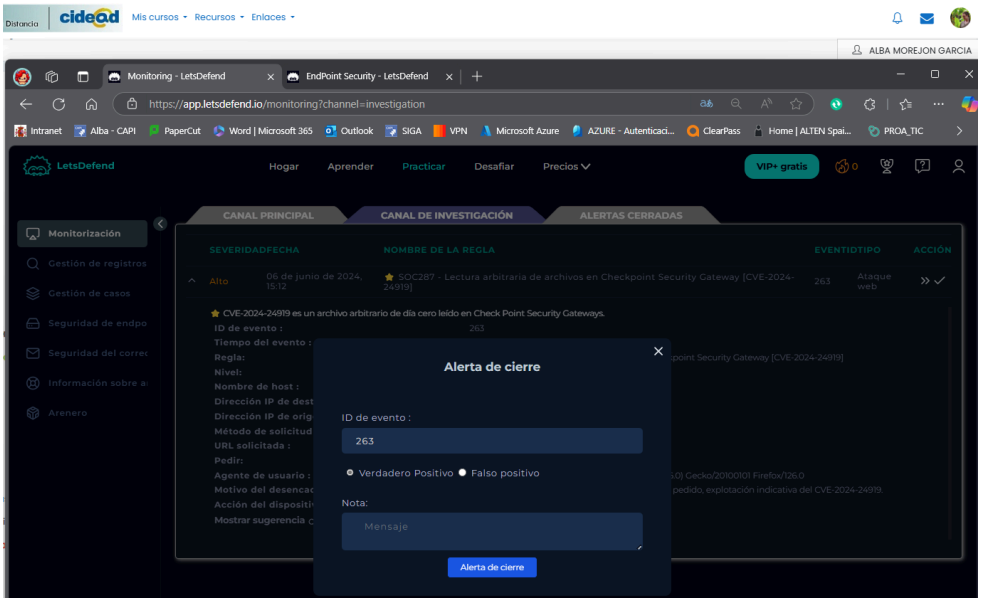
8- Nota del analista

El análisis del incidente ha revelado que el tráfico malicioso detectado es el resultado de un ataque exitoso de Lectura Arbitraria de Archivos (LFI) explotando la vulnerabilidad CVE-2024-24919 en el Check Point Security Gateway. El atacante, utilizando una solicitud HTTP manipulada, logró acceder al archivo /etc/passwd, comprometiendo la seguridad del sistema. La dirección del tráfico malicioso fue desde Internet hacia la red interna, lo que justifica una escalada de nivel 2 para una respuesta más detallada y efectiva. Se han identificado y documentado los artefactos relevantes, y se ha confirmado que el tráfico no es parte de una prueba planificada. Es importante aplicar medidas de mitigación y mantener una comunicación clara con todas las partes involucradas para minimizar el impacto y prevenir futuros incidentes similares.

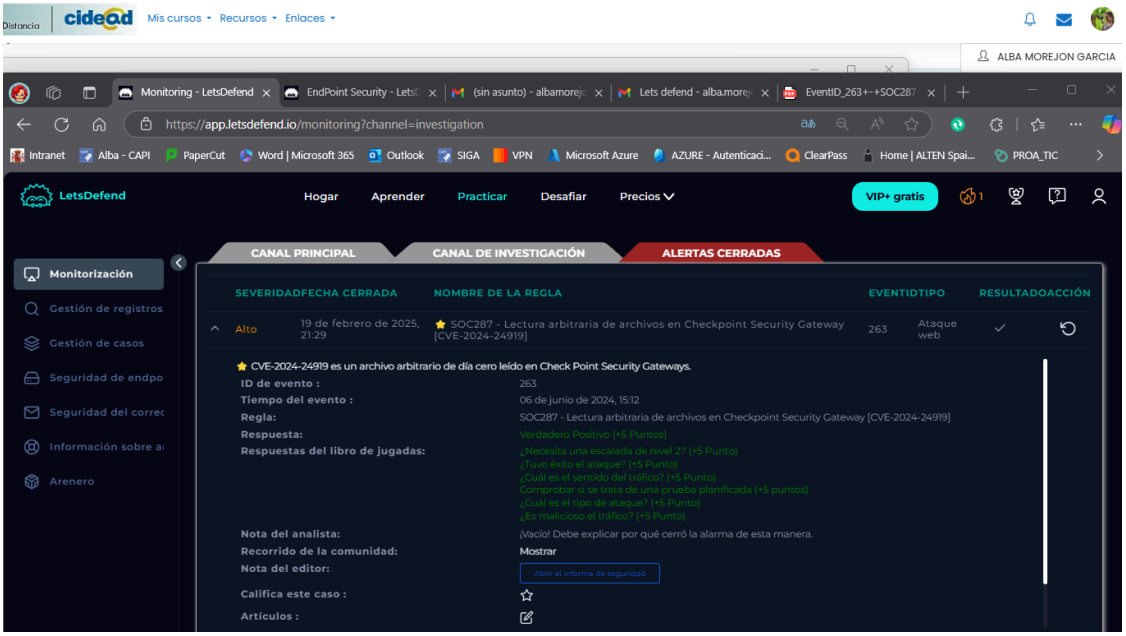


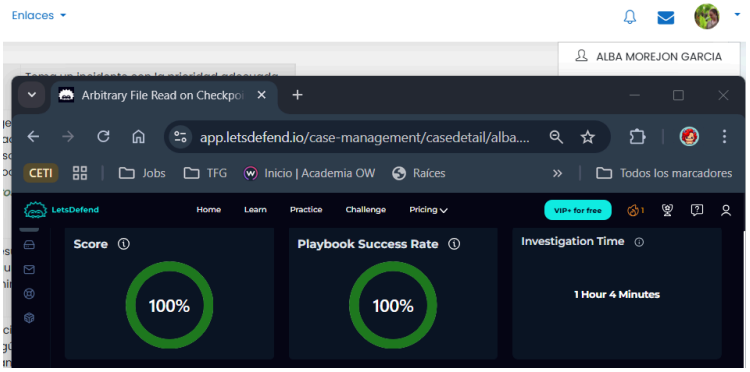
9- Alerta de cierre

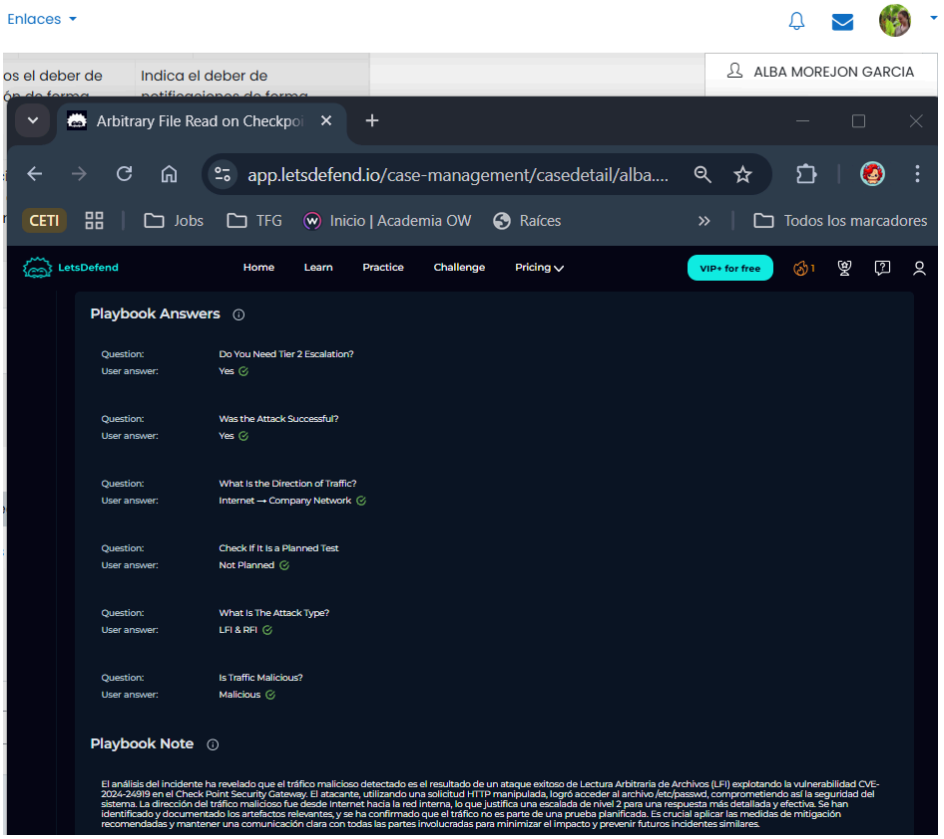
Declaramos que ha sido un verdadero positivo



Resultado:


ALBA MOREJON GARCIA
https://app.letsdefend.io/monitoring?channel=investigation
LetsDefend
Hogar
Aprender
Practicar
Desafiar
Precios
VIP+ gratis
Monitorización
Gestión de registros
Gestión de casos
Seguridad de endpo
Seguridad del correc
Información sobre ai
Arenero
CANAL PRINCIPAL
CANAL DE INVESTIGACIÓN
ALERTAS CERRADAS
SEVERIDADFECHA CERRADA
NOMBRE DE LA REGLA
EVENTIDTIPO
RESULTADOACCIÓN
Alto
19 de febrero de 2025, 21:29
SOC287 - Lectura arbitraria de archivos en Checkpoint Security Gateway [CVE-2024-24919]
263
Ataque web
CVE-2024-24919 es un archivo arbitrario de día cero leído en Check Point Security Gateways.
ID de evento :
263
Tiempo del evento :
06 de junio de 2024, 15:12
Regla:
SOC287 - Lectura arbitraria de archivos en Checkpoint Security Gateway [CVE-2024-24919]
Respuesta:
Verdadero Positivo (+5 Puntos)
Respuestas del libro de jugadas:
¿Necesita una escalada de nivel 2? (+5 Punto)
¿Tuvo éxito el ataque? (+5 Punto)
¿Cuál es el sentido del tráfico? (+5 Punto)
Comprobar si se trata de una prueba planificada (+5 puntos)
¿Cuál es el tipo de ataque? (+5 Punto)
¿Es malicioso el tráfico? (+5 Punto)
Nota del analista:
¡Vacío! Debe explicar por qué cerró la alarma de esta manera.
Recorrido de la comunidad:
Mostrar
Nota del editor:
Abrir el informe de seguridad
Califica este caso :
Artículos :


Enlaces
ALBA MOREJON GARCIA
Arbitrary File Read on Checkpoi
app.letsdefend.io/case-management/casedetail/alba....
CETI
Jobs
TFG
Inicio | Academia OW
Raíces
Todos los marcadores
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Score
100%
Playbook Success Rate
100%
Investigation Time
1 Hour 4 Minutes


Enlaces
os el deber de
Indica el deber de
ALBA MOREJON GARCIA
Arbitrary File Read on Checkpoi
app.letsdefend.io/case-management/casedetail/alba....
CETI
Jobs
TFG
Inicio | Academia OW
Raíces
Todos los marcadores
LetsDefend
Home
Learn
Practice
Challenge
Pricing
VIP+ for free
Playbook Answers
Question:
Do You Need Tier 2 Escalation?
User answer:
Yes
Question:
Was the Attack Successful?
User answer:
Yes
Question:
What Is the Direction of Traffic?
User answer:
Internet → Company Network
Question:
Check If It Is a Planned Test
User answer:
Not Planned
Question:
What Is The Attack Type?
User answer:
LFI & RFI
Question:
Is Traffic Malicious?
User answer:
Malicious
Playbook Note
El análisis del incidente ha revelado que el tráfico malicioso detectado es el resultado de un ataque exitoso de Lectura Arbitraria de Archivos (LFI) explotando la vulnerabilidad CVE-2024-24919 en el Check Point Security Gateway. El atacante, utilizando una solicitud HTTP manipulada, logró acceder al archivo /etc/passwd, comprometiendo así la seguridad del sistema. La dirección del tráfico malicioso fue desde internet hacia la red interna, lo que justifica una escalada de nivel 2 para una respuesta más detallada y efectiva. Se han identificado y documentado los artefactos relevantes, y se ha confirmado que el tráfico no es parte de una prueba planificada. Es crucial aplicar las medidas de mitigación recomendadas y mantener una comunicación clara con todas las partes involucradas para minimizar el impacto y prevenir futuros incidentes similares.

Apartado 2: Comunicaciones de incidentes.
Según el caso práctico planteado con datos ficticios iniciales y del incidente seleccionado se debe realizar la documentación de la notificación y gestión del incidente. Además, se puede añadir toda la información ficticia que se considere necesaria para poder determinar de forma concreta el ciber incidente.
Para la realización de los siguientes apartados se puede consultar la "Guía Nacional de Notificación y Gestión de Ciber Incidentes" en sus apartados 5 y 6.

Deberás efectuar la siguiente tarea:
1. Realizar una clasificación justificada del incidente según la taxonomía oficial.
Categoría del incidente: Ataque web
Subcategoría: Lectura arbitraria de archivos (LFI)
El incidente se clasifica como un ataque web debido a la explotación de la vulnerabilidad CVE-2024-24919 que permite la lectura arbitraria de archivos en los Checkpoint Security Gateways. El atacante utilizó una solicitud HTTP manipulada para acceder al archivo sensible /ect/passwd, comprometiendo la seguridad del sistema.

2. Determinar el nivel de peligrosidad del incidente.
Nivel de peligrosidad: Alto
La vulnerabilidad a la que hemos hecho referencia, es una vulnerabilidad Day Zero que permite a un atacante leer archivos en el sistema afectado. Esto puede llevar a la exposición de información sensible y potencialmente permitir movimientos laterales y escalada de privilegios dentro de la red. La naturaleza crítica del archivo accedido, que contiene información sensible sobre los usuarios del sistema y el hecho de que haya sido permitido y no bloqueado por el sistema, aumenta la peligrosidad del incidente. La explotación de esta vulnerabilidad compromete la integridad y confidencialidad de los datos

3. Determinar el nivel de impacto del ciber incidente.
Nivel de impacto: Crítico
La explotación de la vulnerabilidad CVE-2024-24919 puede comprometer datos confidenciales y afectar la integridad y confidencialidad de la información en los sistemas (sede ministerial de Justicia en Andalucía). Además, puede tener repercusiones legales y de reputación significativas. La capacidad del atacante para acceder al archivo sugiere que la seguridad del sistema ha sido gravemente comprometida.

4. Indicar la posible obligación de notificar al CSIRT correspondiente.
Obligación de notificación: si
Según la Guía Nacional de Notificación y Gestión de Ciberincidentes, los incidentes que comprometen la seguridad de la información en entidades públicas deben ser notificados al CSIRT correspondiente. Dado el nivel de peligrosidad y el impacto de este incidente, es obligatorio notificar al INCIBE-CERT (Instituto Nacional de Ciberseguridad de España) para coordinar la respuesta y la mitigación, ya que el incidente involucra una brecha de seguridad significativo que afecta a una entidad pública.

5. Rellenar una tabla con la información que se enviaría al CSIRT.

CAMPO	DETALLE
Fecha y hora del incidente	06 de junio de 2024, 03:12 pm
Nombre del incidente	Lectura arbitraria de archivos en Checkpoint Security Gateway (CVE-2024-24919)
Descripción del incidente	Explotación de una vulnerabilidad de día cero que permite la lectura arbitraria de los archivos, accediendo al archivo /etc/passwd mediante una solicitud HTTP POST con payload malicioso
Nivel de peligrosidad	Alto
Nivel de impacto	Crítico
IP de origen	203.160. 68,12
IP de destino	172.16.20.146
Nombre del host	CP-Sark-Gateway-01
Modo de ataque	Solicitud HTTP POST con payload malicioso para leer el archivo /etc/password
Impacto	Compromiso de datos confidenciales y posible escalada de privilegios
Medidas tomadas	Contención del host, análisis de artefactos, escalada a nivel 2, aplicación del hotfix proporcionado por Check Point, monitoreo continuo del sistema…
Contacto	Nombre del responsable de seguridad, email y teléfono

6. Explicar cuantas notificaciones son requeridas y con qué frecuencia. (No hay que crear las notificaciones)

Número de notificaciones requeridas: Múltiples, para asegurar una gestión efectiva del incidente.
Frecuencia:

- Inicial: notificación inmediata al detectar y confirmar el incidente. Se deben proporcionar detalles clave sobre el incidente, para alertar al CSIRT y coordinar una respuesta rápida.
- Actualización: notificaciones periódicas cada 24 horas o según el progreso del incidente, hasta la resolución completa. Deben incluir cualquier cambio significativo en el estado del incidente, nuevas evidencias, medidas adicionales y el progreso para la mitigación del ataque. La frecuencia de las actualizaciones se ajustará según las indicaciones del CSIRT y la gravedad del incidente.
- Final: notificación de cierre, una vez que el incidente ha sido mitigado y resuelto. Se debe resumir todas las acciones tomadas, los resultados obtenidos y cualquier aportación útil para futuros incidentes (lecciones aprendidas).

Este proceso de notificación asegura que todas las partes involucradas estén informadas y que se tomen las medidas adecuadas para proteger la seguridad de la red y los datos de la organización.

7. Rellenar la información con el estado del cierre del incidente.

Estado del cierre: cerrado
El incidente se cerrará una vez que se hayan completado todas las acciones de mitigación y se haya confirmado que no hay más amenazas activas. En este caso, el incidente ha sido mitigado mediante la contención del host afectado y la implementación de medidas de seguridad adicionales (aplicación de hotfix). Se ha realizado un monitoreo exhaustivo para asegurar que no haya más intentos de explotación de la vulnerabilidad. Todo el proceso ha sido documentado, incluyendo las lecciones aprendidas y las recomendaciones para prevenir futuros incidentes similares. La información se ha desarrollado según las indicaciones de la Guía Nacional de Notificaciones y Gestión De Incidentes.