LA CUEVA

BLUE TEAM

EXPEDIENTE DE INVESTIGACIÓN

El equipo que nadie podía explicar

Preparación informática / Sistemas / Acceso GRATUITO

Resolver, justificar y comunicar. Este pack es breve, editable y está pensado para producir una evidencia de trabajo reutilizable.

Formato: briefing · entorno seguro · preguntas · informe profesional

Aprender a investigar con evidencia.

01 / Contexto de misión

Leé el caso antes de consultar el entorno. Separá hechos, hipótesis y datos que todavía faltan.

Campo	Información
Ticket	HELP-1007 · Notebook lenta y proceso desconocido
Nivel	Preparación informática
Dificultad	Inicial
Duración	35-45 min
Afectado	COMPRAS-07 · Usuario de Compras
Alerta	Endpoint: proceso no reconocido

Situación

Asteria Logistics recibe el ticket HELP-1007: LAP-FIN-042 está lenta desde la mañana. Lucía Ferrer menciona una carpeta llamada _backup_old y un proceso llamado sync-helper, pero no sabe si forman parte del equipo. No hay indicios suficientes para afirmar un incidente.

Objetivo

- Identificar un activo y su contexto.
- Distinguir observación de conclusión.
- Documentar rutas, procesos y permisos.

Antes de empezar

- Saber usar un explorador de archivos.
- Reconocer usuario, proceso y carpeta.

02 / Entorno controlado

Explorá una imagen ficticia de solo lectura y escribí cualquier comando que te ayude a investigar. La entrada se interpreta dentro del caso; no ejecuta procesos reales, toca tu equipo ni realiza conexiones externas.

Archivo virtual	Qué buscar
case-notes.txt	Hechos, fuente, tiempo y datos que todavía faltan.
evidence-index.txt	Hechos, fuente, tiempo y datos que todavía faltan.
timeline.txt	Hechos, fuente, tiempo y datos que todavía faltan.
readme.txt	Hechos, fuente, tiempo y datos que todavía faltan.

Fuentes disponibles

Archivo / consulta	Qué buscar
01 · Ticket	Actor, origen, timestamp y relación con la hipótesis.
02 · Inventario	Actor, origen, timestamp y relación con la hipótesis.
03 · Procesos	Actor, origen, timestamp y relación con la hipótesis.
04 · Permisos	Actor, origen, timestamp y relación con la hipótesis.

Regla de oro

Un comando puede aportar un indicio, pero no reemplaza la correlación con el ticket, el activo, el usuario y el momento. No descargues muestras ni uses credenciales reales.

03 / Preguntas de evidencia y análisis

Respondé con hechos, fuente, timestamp, hipótesis y limitaciones. Si no podés confirmarlo, escribí qué dato pedirías.

01 · ¿Qué datos mínimos del equipo y del usuario registrarías primero?

Respuesta editable

02 · ¿Qué diferencia hay entre un proceso desconocido y un proceso malicioso?

Respuesta editable

03 · ¿Qué permisos y rutas revisarías sin modificar nada?

Respuesta editable

04 · ¿Qué próximo paso seguro dejarías documentado para otro analista?

Respuesta editable

04 / Informe profesional

Este documento debe permitir que otro analista retome el caso sin una explicación oral. Completalo después de usar el entorno.

Resumen ejecutivo · qué pasó y por qué importa

Hechos y evidencia · fuente + hora

Hipótesis · alternativa + nivel de confianza

Impacto, contención y próximo paso

Checklist de entrega

- Separé hechos, inferencias y datos pendientes.
- No afirmé ejecución o compromiso sin evidencia.
- Escribí impacto, contención y limitaciones.
- El siguiente paso tiene dueño y validación.

Entregable para portfolio

- Inventario de endpoint en una página.
- Tabla de observables y fuentes.
- Hipótesis con nivel de confianza.
- Siguiente consulta segura.