LA CUEVA

BLUE TEAM

EXPEDIENTE DE INVESTIGACIÓN

La conversación que no debía salir

Redes / Network / 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	NET-1012 · Consultas DNS periódicas
Nivel	Redes
Dificultad	Inicial
Duración	50-70 min
Afectado	PATIO-03 · Red de invitados
Alerta	DNS: patrón periódico fuera de horario

Situación

El equipo PATIO-03 aparece en un ticket de monitoreo porque resuelve api-metricas.example cada 60 segundos durante la madrugada. La empresa tiene una aplicación de analítica que genera consultas frecuentes, aunque el inventario no confirma si está instalada en ese equipo.

Objetivo

- Leer origen, destino y protocolo.
- Seguir una resolución DNS y su conexión posterior.
- Comparar anomalía y uso legítimo.

Antes de empezar

- Reconocer DNS, IP, puerto y flujo.
- Conocer filtros básicos de Wireshark.

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 · PCAP	Actor, origen, timestamp y relación con la hipótesis.
02 · DNS logs	Actor, origen, timestamp y relación con la hipótesis.
03 · Inventario	Actor, origen, timestamp y relación con la hipótesis.
04 · Ticket	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 · ¿Quién consulta a quién y con qué protocolo?

Respuesta editable

02 · ¿Qué rasgos del flujo son observables y cuáles son solo hipótesis?

Respuesta editable

03 · ¿Qué filtro usarías para seguir la conversación en la captura?

Respuesta editable

04 · ¿Qué evidencia pedirías antes de bloquear el dominio?

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

- Timeline DNS.
- Tabla de IOC con confianza.
- Comparación de hipótesis.
- Recomendación sin bloqueo ciego.