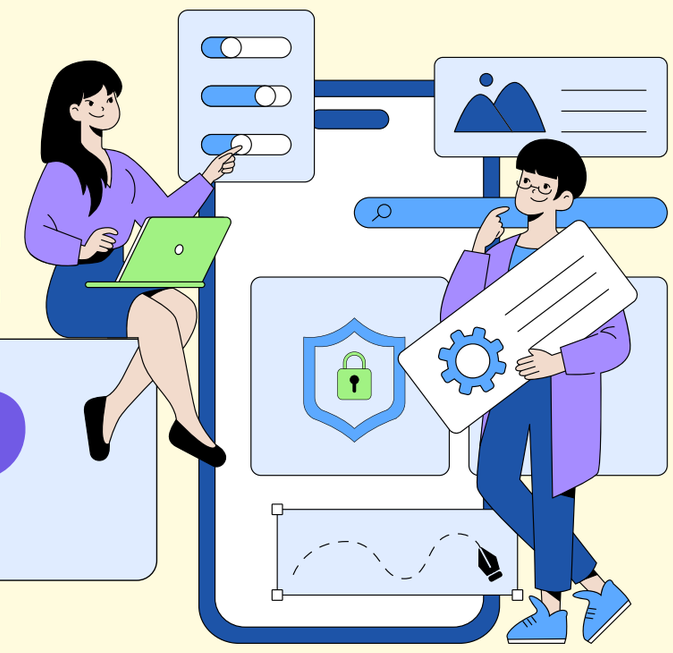
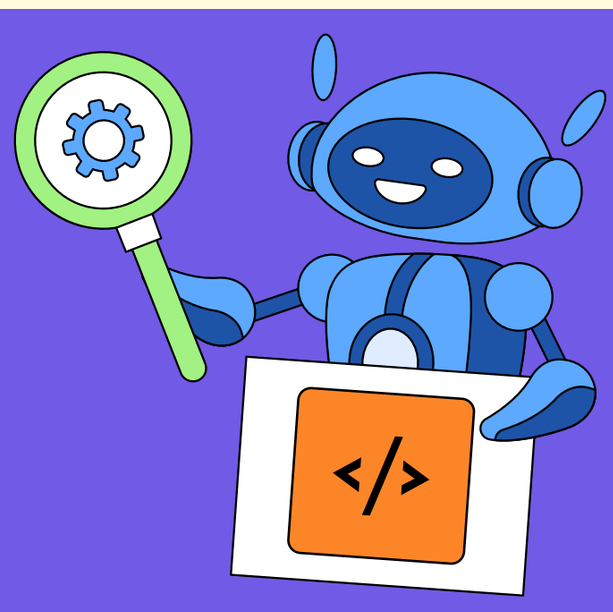
GUÍA PARA CONTRARRESTAR INCIDENTES DE

SINKHOLE HTTP

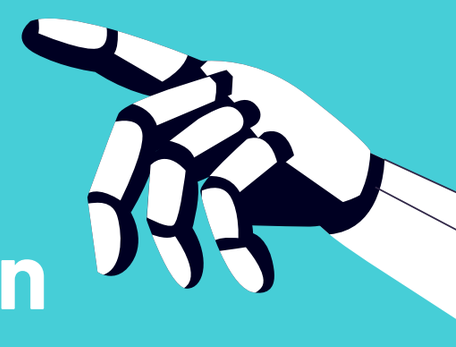


Introducción

Un Sinkhole HTTP **redirige conexiones maliciosas** hacia servidores controlados para monitoreo, análisis o mitigación de amenazas.



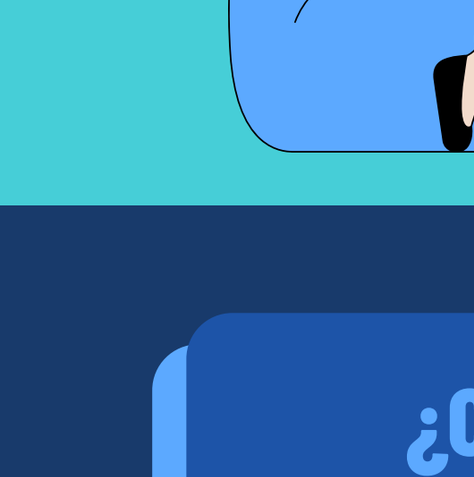
¿Qué es un Sinkhole HTTP?



Es un mecanismo que **desvía tráfico HTTP sospechoso a un servidor seguro** para identificar equipos comprometidos.

¿Cómo funciona?

Redirige conexiones maliciosas e identifica equipos comprometidos mediante análisis de tráfico.

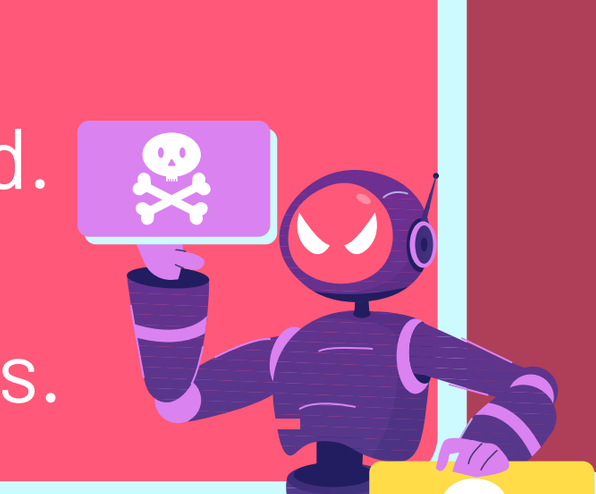


Riesgos asociados

- Persistencia de
- Movimiento lateral en la red.
- Exposición de datos sensibles.

Pasos para Contrarrestar el Incidente

1. Identificar conexiones Sinkhole HTTP
2. Analizar el equipo comprometido
3. Contener el incidente
4. Erradicar la amenaza
5. Fortalecer la seguridad
6. Monitoreo continuo



Recomendaciones

Capacitar al personal técnico, mantener inventario de dominios sinkhole y configurar alertas en el SIEM corporativo.

ecucert
Centro de respuesta a incidentes informáticos del Ecuador

EL NUEVO ECUADOR