# README – Ransomware Network Detection Demo

Repositorio de muestras de tráfico (PCAP) y recursos para entrenar detección de ransomware exclusivamente a través de análisis de red.

## 🔎 ¿Qué incluye este repositorio?

- 3 archivos PCAP simulados: tráfico limpio, cifrado vía SMB, y exfiltración DNS.

- Descripción técnica de cada captura.

- Reglas sugeridas para Zeek y Suricata (ver recursos adicionales).

## 📁 Estructura del Repositorio

ransomware-network-detection-demo/  
├── pcap\_samples/  
│ ├── smb\_encryption.pcapng  
│ ├── dns\_exfiltration.pcapng  
│ ├── clean\_traffic.pcapng  
├── pcap\_descriptions.md  
├── README.md  
├── LICENSE (opcional)

## 💡 Cómo usarlo

- Analizá los PCAPs con Wireshark, Zeek o Suricata.

- Buscá patrones de cifrado, exfiltración o comportamiento anómalo.

- Ideal para ejercicios de detección o entrenamiento blue team.

## ✍️ Autor

GitHub: https://github.com/thc3pt3r  
Proyecto educativo y abierto para la comunidad IR/Blue Team.