# MSI Threat Intelligence & Blue Team Tool


**Resumen de Funcionalidades:**

**Threat Intelligence (Inteligencia de Amenazas):**

**Obtención de Datos de Amenazas:**

- La herramienta puede obtener información de amenazas desde diversas fuentes, incluyendo ExploitDB, NIST NVD y CVE MITRE.

**Análisis de Amenazas:**

- Proporciona capacidades de análisis básico y avanzado de amenazas.
- Detecta patrones específicos y categoriza amenazas en función del contenido proporcionado.

**Blue Team (Equipo de Blue Team):**

**Respuesta a Incidentes:**

- Ofrece una serie de acciones avanzadas para responder a incidentes de seguridad.
- Puede desconectar remotamente dispositivos comprometidos.
- Permite el cifrado de datos sensibles.
- Registra incidentes en un archivo de registro local.
- Notifica a las autoridades en caso de amenazas graves.
- Cifrado de Datos:
- Puede cifrar datos sensibles según las necesidades del caso.

**Desconexión Remota de Dispositivos:**

- Permite desconectar dispositivos remotos mediante la introducción de la dirección IP del dispositivo objetivo.

**Registro de Incidentes:**

- Registra incidentes de seguridad en un archivo de registro local para futuras referencias y análisis.

**Notificación a las Autoridades:**

- Notifica a las autoridades en caso de amenazas graves o incidentes críticos de seguridad.

**Funciones Adicionales:**

**Interfaz Gráfica de Usuario (GUI):**

- La herramienta cuenta con una interfaz gráfica que facilita su uso.

**Envío de Correos Electrónicos:**

- Puede enviar correos electrónicos a destinatarios específicos, útil para notificar a las autoridades o partes interesadas.

**Categorización de Amenazas:**

- Clasifica las amenazas detectadas en categorías como malware, phishing, ataques de fuerza bruta, etc.

**Encriptación de Datos:**

- Utiliza la biblioteca Fernet para cifrar datos sensibles.

**Descargo de Responsabilidad:**

- Incluye un descargo de responsabilidad que prohíbe el uso comercial de la herramienta sin permiso del creador.

**Cómo Usar la Herramienta:**

La herramienta se inicia mediante la interfaz gráfica.

Hay dos pestañas principales: "Threat Intelligence" y "Blue Team".

En "Threat Intelligence", se pueden obtener y analizar datos de amenazas.

En "Blue Team", se pueden realizar acciones de respuesta ante incidentes y cifrado de datos.

La herramienta puede desconectar dispositivos remotos, cifrar datos sensibles y notificar a las autoridades en caso de amenazas graves.

También puede registrar incidentes en un archivo de registro local.

**La herramienta está diseñada para su uso en entornos de seguridad y Blue Team, proporcionando capacidades de análisis y respuesta ante amenazas de seguridad de forma efectiva y personalizable. Asegúrate de configurar adecuadamente las funciones de correo electrónico y desconexión remota según tus necesidades específicas.**