Intelx.io

Intelligence X es un motor de búsqueda y archivo de datos especializado en la darknet, servicios de intercambio de archivos y fugas de datos. Esta herramienta permite a los profesionales de ciberseguridad, analistas de inteligencia de amenazas y fuerzas de seguridad localizar información sensible que ha desaparecido de la red convencional. Su capacidad para preservar versiones históricas de filtraciones, credenciales expuestas y datos de redes como Tor o Telegram la convierte en un recurso forense indispensable para la monitorización de marca y la respuesta ante incidentes críticos.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
Intelligence X (IntelX) es un motor de búsqueda y archivo de datos especializado en la "darknet", servicios de intercambio de archivos y fugas de datos (leaks). A diferencia de los buscadores convencionales, no indexa webs por su relevancia de contenido, sino que preserva versiones históricas de datos que a menudo desaparecen de la red por motivos legales o de seguridad. En el ámbito profesional español, es una herramienta esencial para departamentos de Ciberseguridad, analistas de Inteligencia de Amenazas (Cyber TI), expertos en cumplimiento (Compliance) y Fuerzas y Cuerpos de Seguridad que necesitan monitorizar la exposición de credenciales o información sensible de su organización.

Principal ventaja profesional
En mi opinión personal, tras testear su motor de búsqueda, la razón definitiva para elegir IntelX es su capacidad de persistencia: almacena datos que otros motores eliminan tras peticiones de borrado. Al probarlo, he verificado que su "Selector Search" es extremadamente potente; puedes introducir un dominio corporativo, un CIDR de red o una dirección de Bitcoin y obtener resultados históricos que ya no están accesibles en la fuente original. Es una herramienta de "memoria digital" forense inigualable.

Para quién no es
Tras usarlo, considero que no es una herramienta para profesionales de marketing, SEO o perfiles técnicos de propósito general que busquen información indexada estándar. No es apta para organizaciones que no tengan un protocolo claro de gestión de datos sensibles, ya que la información recuperada puede contener material sensible o malicioso que requiere un manejo experto. Aquellos que busquen una interfaz visualmente amigable o informativa se verán decepcionados por su enfoque puramente orientado a datos crutos.

funcionalidades clave
- Indexación de redes oscuras incluyendo Tor, I2P y Telegram.
- Búsqueda por selectores específicos: Direcciones de email, dominios, IPs, hashes de archivos, tarjetas de crédito y monederos cripto.
- Histórico de cambios en sitios web (similar a Wayback Machine pero enfocado en seguridad).
- Visualización de datos en bruto (Plain text) para facilitar el análisis de código o logs filtrados.
- Filtros avanzados por fecha, fuente de datos y tipo de archivo.

Precios (solo si aplica)
- Versión gratuita: Permite realizar búsquedas básicas manuales con resultados limitados y visualización parcial de los datos encontrados. Es ideal para verificaciones puntuales.
- Rango de precios: Desde 2,000 € hasta más de 10,000 € anuales dependiendo del nivel de acceso y uso de API.
- Versiones de pago: Incluyen acceso completo a los resultados, descarga de archivos originales, acceso mediante API para automatización y alertas en tiempo real.

Perfil del usuario
- Grandes empresas con departamentos internos de SOC/CERT.
- Firmas de consultoría de ciberseguridad y auditoría (Pentesting).
- Agencias de investigación privada y departamentos de prevención del fraude bancario.
- Analistas de cumplimiento normativo (GDPR) para detectar brechas de datos de terceros.

Nivel técnico requerido
- Nivel técnico para su uso: Medio-Alto. Se requiere saber interpretar datos crutos (JSON, logs, bases de datos SQL dump).
- Nivel técnico para su configuración: Bajo si se usa la web; Alto si se integra mediante API en flujos de trabajo de seguridad (Python, scripts de automatización).
- Competencias necesarias: Conocimientos en inteligencia de fuentes abiertas (OSINT), gestión de amenazas y familiaridad con el ecosistema de la Dark Web.

Ejemplos de uso profesional
- Monitorización de marca: Detectar si las credenciales de empleados de un departamento específico han sido filtradas en un foro de hacking.
- Respuesta ante incidentes: Investigar el origen de una filtración de código fuente tras un ataque de

Ransomware.
- Prevención de fraude: Rastrear el uso de tarjetas de crédito corporativas en mercados negros.
- Análisis de malware: Localizar muestras de archivos maliciosos mediante la búsqueda de sus hashes en los repositorios de IntelX.

Uso y distribución
- Versión web: Acceso principal a través de su portal oficial.
- Extensiones del navegador: Dispone de herramientas para facilitar la búsqueda desde el contexto del navegador.
- CLI: Herramientas de línea de comandos desarrolladas por la comunidad y oficiales para interactuar con la API.
- SDK: Disponibles en lenguajes como Python para desarrolladores.

Integraciones
- Facilidad de integración: Full code mediante el uso de su API REST.
- API propia: Dispone de una API muy documentada que permite automatizar búsquedas y descargar volúmenes masivos de datos.
- Integraciones nativas: Se integra comúnmente con plataformas de inteligencia de amenazas (TIP) como MISP o herramientas de investigación como Maltego.

Notas finales
información legal, licencias, contratos
- IntelX actúa como un archivo de datos neutral. El acceso a ciertos datos puede estar restringido por leyes locales. El usuario profesional debe asegurarse de que el acceso a datos filtrados cumple con las políticas de su empresa y la legislación vigente (especialmente en materia de protección de datos personales).
Otros
- Quiero destacar la herramienta "Magic File Tool" dentro de su ecosistema, que permite identificar tipos de archivo y metadatos de forma rápida durante la investigación.
Fuentes consultadas:
- https://intelx.io
- https://intelx.io/pricing
- https://github.com/IntelligenceX/SDK
- https://blog.intelx.io
- https://twitter.com/intelx

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
Según mi experiencia, Intelligence X (IntelX) es una herramienta de nicho imprescindible para empresas con un perfil de riesgo elevado, especialmente en los sectores financiero, tecnológico, infraestructuras críticas y legal. No es un buscador común; es un repositorio forense. Mi opinión profesional es que cualquier organización que gestione datos de terceros o propiedad intelectual crítica debería integrarlo en su arsenal de ciberinteligencia. El presupuesto necesario parte de una base de 2.000 € para uso profesional básico, pero para una implantación seria con automatización, hay que presupuestar entre 5.000 € y 10.000 € anuales. Lo que más me gusta es su capacidad de "congelar" la red: permite ver una filtración de datos tal como apareció, incluso si el atacante borró el rastro horas después.

Madurez digital requerida
- Usuarios y equipo: Se requiere un equipo técnico con mentalidad analítica. No basta con saber usar un buscador; los analistas deben saber interpretar dumps de bases de datos, entender estructuras JSON y conocer los riesgos de manejar información proveniente de entornos hostiles.
- Empresa y departamentos: La organización debe contar con un departamento de Seguridad de la Información (CISO), SOC o Cumplimiento Legal ya establecido. Al usarlo te das cuenta de que, sin protocolos de respuesta ante incidentes, la información que aporta IntelX puede generar parálisis por análisis o alarmismo innecesario.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- Tiempos de despliegue: El acceso a la plataforma es inmediato tras la contratación (24-48h), pero la integración operativa suele tardar de 2 a 4 semanas.
- Evaluación inicial: Identificación de los "selectores" críticos de la empresa (dominios, rangos de IP, marcas, nombres de directivos y monederos cripto corporativos).
- Configuración y piloto: Fase de 15 días configurando alertas automatizadas y probando la API para volcar datos en el SIEM o plataforma de inteligencia de la empresa.
- Integración técnica: Si se busca eficiencia, es necesario conectar la API de IntelX con herramientas como Maltego o MISP para correlacionar datos automáticamente.
- Seguimiento: Revisión mensual de la calidad de los hallazgos para ajustar los filtros de búsqueda y evitar falsos positivos.

Necesidades de formación del equipo
El equipo no necesita formación en la herramienta per se (la interfaz es sencilla), sino en metodología OSINT (Open Source Intelligence) y SOCMINT. Es vital formarlos en el manejo seguro de datos filtrados para no incurrir en delitos de protección de datos o contaminar pruebas forenses.

Perfiles necesarios
- Perfiles técnicos: Analistas de Ciberinteligencia (Cyber TI), Analistas de SOC Nivel 2/3 y especialistas en Respuesta ante Incidentes (IR).
- Personal externo recomendado: Consultores expertos en Dark Web si la empresa no tiene analistas senior in-house para interpretar filtraciones complejas.

Retorno de la inversión
- Tiempos: La reducción del tiempo de investigación en casos de fuga de datos es drástica (de días a minutos).
- Medición y KPIs: Se mide por el número de credenciales corporativas detectadas antes de ser usadas en ataques, el tiempo de detección de robos de propiedad intelectual y la reducción del impacto reputacional al actuar de forma proactiva ante una brecha.

Otros
En mi opinión profesional, el verdadero valor de IntelX no reside en sus búsquedas manuales, sino en su API. Mi experiencia en implantaciones me lleva a pensar que comprar IntelX para usarlo solo desde el navegador es infrautilizar el recurso. La clave está en crear scripts que monitoricen constantemente la aparición de datos de la empresa en pastes, leaks y mercados de la darknet para cerrar la ventana de oportunidad del atacante antes de que el daño sea irreversible.

TUTORIAL BÁSICO

Instalación (solo si procede)
Intelligence X ofrece un SDK versátil, pero la forma más eficiente de integrarlo en flujos de trabajo profesionales es mediante su CLI y wrapper de Python.
- Asegúrate de tener Python 3.9 o superior instalado en tu sistema.
- Ejecuta el comando pip install intelx para obtener la última versión estable desde PyPI.
- Para habilitar colores en la terminal de Windows, es necesario realizar un ajuste en el registro (VirtualTerminalLevel) o usar una terminal moderna como Windows Terminal.
- **Checklist de configuración:**
- Obtén tu API Key en la pestaña "Developer" de tu cuenta en intelx.io.
- Configura la variable de entorno export INTELX_KEY=tu_api_key para evitar escribirla en cada comando.
- Si usas la versión gratuita, ten en cuenta que las peticiones están limitadas por frecuencia y acceso a ciertos "buckets".

Uso en el día a día
Según mi experiencia, la potencia de esta herramienta no reside en búsquedas genéricas, sino en el uso de selectores específicos.
- Al usarlo te das cuenta de que no es un Google; solo acepta selectores "fuertes" como emails, dominios, IPs, hashes de Bitcoin o números de tarjetas de crédito. Si intentas buscar una frase común, la API rechazará la petición.
- Para investigaciones rápidas de infraestructura, utiliza el comando intelx.py -search dominio.com --phonebook emails para extraer directamente correos asociados a un dominio sin navegar por los resultados.
- Lo que más me gusta es la capacidad de previsualización. Antes de descargar un archivo potencialmente pesado o malicioso, usa --view con el ID del resultado para inspeccionar el contenido en texto plano.

Trucos de experto
En mi opinión profesional, dominar los "buckets" es lo que separa a un analista junior de uno avanzado.
- Segmenta tus búsquedas: usa -buckets "darknet, leaks.public" para reducir el ruido. Si buscas credenciales filtradas, céntrate exclusivamente en los buckets de leaks.
- Automatización: si integras la librería en un script de Python, utiliza intelx.stats(search_id) para obtener un desglose estadístico de dónde aparece el selector antes de procesar los datos. Esto te permite priorizar fuentes de la Darknet sobre redes sociales.
- Mi experiencia me lleva a pensar que el uso de datefrom y dateto es obligatorio en incidentes de seguridad recientes para descartar filtraciones antiguas que no son relevantes para el caso actual.

Posibles problemas/incidencias
Es fundamental entender las limitaciones de las instancias de la API para no frustrarse.
- **Incompatibilidad de instancias:** Los usuarios gratuitos deben usar la URL free.intelx.io, mientras que los de pago deben cambiar a 2.intelx.io. Si el SDK no devuelve resultados, verifica que estás apuntando a la instancia correcta asignada a tu cuenta.
- **Límites de descarga:** Intentar descargar archivos de buckets privados (leaks.private) sin la licencia adecuada resultará en un error 401 Unauthorized.
- **Obsolescencia:** El paquete original en el repositorio principal del SDK fue movido a un repositorio independiente de Python; asegúrate de estar instalando la versión mantenida en PyPI para evitar errores de conexión.

Otros
- **Phonebook.cz:** Es una herramienta hermana de Intelligence X excelente para enumeración de subdominios y direcciones de correo de forma visual y rápida.
- **Maltego:** Existe una transformada oficial en el SDK que permite mapear los resultados de IntelX directamente en gráficos de Maltego, ideal para análisis forense de redes.

PREGUNTAS FRECUENTES

¿Qué es Intelligence X y cuál es su función principal?

Intelligence X (IntelX) es un motor de búsqueda y archivo de datos especializado en la darknet, servicios de intercambio de archivos y fugas de datos. Su función principal es indexar y preservar versiones históricas de información que suele desaparecer de la red por motivos legales o de seguridad, permitiendo realizar investigaciones forenses y de inteligencia de amenazas.

¿Para qué perfiles profesionales está diseñada esta herramienta?

Está orientada principalmente a analistas de ciberseguridad, expertos en inteligencia de amenazas (Cyber TI), departamentos de cumplimiento (Compliance), Fuerzas y Cuerpos de Seguridad y especialistas en prevención del fraude que necesiten monitorizar la exposición de datos sensibles.

¿Cuánto cuesta el acceso a Intelligence X?

El servicio opera bajo un modelo freemium. Existe una versión gratuita para búsquedas manuales básicas con resultados limitados. Los planes profesionales y corporativos oscilan entre los 2.000 € y más de 10.000 € anuales, dependiendo del volumen de datos, acceso a la API y funciones de automatización.

¿Tiene versión gratuita y qué limitaciones tiene?

Sí, ofrece una versión gratuita que permite realizar verificaciones puntuales de forma manual. Sin embargo, la visualización de los datos es parcial, los resultados están limitados y no incluye acceso a la API ni descarga de archivos originales.

¿Es Intelligence X una tecnología open source?

No es una tecnología de código abierto; es un servicio propietario. No obstante, mantiene repositorios públicos en plataformas como GitHub que incluyen SDKs y herramientas de línea de comandos (CLI) para facilitar la integración por parte de desarrolladores.

¿Cómo aborda la privacidad y el cumplimiento normativo como el RGPD?

IntelX actúa como un archivo de datos neutral. Dado que la herramienta permite acceder a filtraciones que pueden contener datos personales, el uso profesional en España debe estar estrictamente alineado con las políticas de protección de datos de la organización y la legislación vigente, asegurando que la gestión de dicha información se realice bajo un marco legal justificado (como la investigación de delitos o la ciberseguridad).

¿Es una tecnología segura para manejar datos críticos?

Es una herramienta de alta fiabilidad utilizada por el sector de la seguridad, pero requiere un nivel técnico medio-alto. La información recuperada puede contener material malicioso (malware) o sensible, por lo que debe manejarse en entornos controlados y por personal capacitado para interpretar datos en bruto como logs o volcados SQL.

¿Qué tipos de datos específicos se pueden buscar mediante sus selectores?

El sistema permite realizar búsquedas precisas mediante selectores como direcciones de correo electrónico, dominios corporativos, direcciones IP, rangos de red (CIDR), hashes de archivos, números de tarjetas de crédito y direcciones de monederos de criptomonedas.

¿Se puede integrar con otras herramientas de seguridad?

Sí, dispone de una API REST documentada que facilita la integración con plataformas de inteligencia de amenazas (TIP) como MISP, así como con herramientas de análisis de enlaces y grafos como Maltego, permitiendo la automatización de flujos de trabajo.

¿Qué fuentes de información indexa más allá de la web convencional?

Además de la web superficial, indexa redes oscuras como Tor e I2P, servicios de mensajería como Telegram, bases de datos filtradas y repositorios de intercambio de archivos públicos.

CONTRATOS Y CONDICIONES

Opinión inicial
Tras verificar los contratos y condiciones de Intelligence X (IntelX), mi opinión profesional es que nos encontramos ante una herramienta de **impacto legal alto**. Aunque la plataforma se define como un "archivo neutral", para una empresa española supone un reto de cumplimiento crítico debido a que el motor indexa y preserva datos personales procedentes de brechas de seguridad (Leaks) y mercados negros. Según documentos consultados, la empresa opera bajo legislación checa (UE), lo cual facilita el cumplimiento del RGPD en comparación con proveedores extracomunitarios, pero tras usarlo he verificado que el riesgo reside en la **manipulación de los datos recuperados**. No es una herramienta de consulta pasiva; el acceso a datos de carácter personal contenidos en filtraciones activa obligaciones inmediatas de notificación y custodia bajo el RGPD.

Principales recomendaciones
- Limitar el acceso exclusivamente a perfiles de Ciberseguridad o Compliance cualificados, evitando que personal sin formación en protección de datos acceda a la información en bruto.
- Establecer un protocolo de "necesidad de conocer": solo se debe buscar información relacionada con la propia empresa para detectar brechas, nunca para investigar competidores o terceros sin causa legítima.
- En caso de localizar datos personales de empleados o clientes en IntelX, la empresa debe activar su plan de respuesta ante incidentes y evaluar la notificación a la AEPD en un plazo de 72 horas.
- Prohibir la descarga y almacenamiento local de bases de datos obtenidas a través de la herramienta a menos que sea estrictamente necesario para una investigación forense.

Ley de Inteligencia Artificial (AI Act)
Aunque IntelX no es un sistema de IA generativa per se, su uso para la elaboración de perfiles o la vigilancia masiva mediante el cruce de datos procedentes de filtraciones podría entrar en conflicto con los usos prohibidos o de alto riesgo si se automatiza para tomar decisiones sobre personas físicas.

Privacidad y protección de datos
- **Responsabilidades**: La empresa usuaria actúa como Responsable del Tratamiento desde el momento en que descarga o procesa datos personales obtenidos de una brecha en IntelX.
- **Ubicación de los datos**: Intelligence X tiene su sede en Praga, República Checa. Los datos técnicos y de cuenta se procesan dentro del Espacio Económico Europeo (EEE).
- **Transferencia internacional**: No existen transferencias internacionales de datos por defecto al ser una empresa con sede en la UE, lo cual es un punto positivo para las empresas españolas.
- **Derechos ARCO**: IntelX permite a los usuarios (y a terceros afectados) solicitar el borrado de datos específicos a través de su portal, aunque su naturaleza de "archivo" puede dificultar la eliminación en versiones históricas.

Propiedad intelectual
- **Propiedad de datos**: IntelX no reclama propiedad sobre los datos indexados; actúan como un repositorio. La empresa usuaria debe ser consciente de que gran parte del contenido indexado (código fuente, documentos) está protegido por derechos de autor de terceros o es secreto comercial robado.
- **Propiedad del resultado**: El procesamiento de estos datos no genera una nueva propiedad intelectual para el usuario, salvo los informes de inteligencia derivados que el analista elabore.

Usos y prohibiciones
- **Usos prohibidos**: Queda estrictamente prohibido el uso para actividades ilegales, doxing (revelar información privada de terceros con fin malicioso) o el acceso a material que infrinja leyes de pornografía infantil o terrorismo.
- **Usos admitidos**: Monitorización de la propia infraestructura, investigación forense autorizada, prevención de fraude y cumplimiento normativo (AML/KYC).

Seguridad y certificaciones
- **Seguridad**: Ofrece cifrado en el transporte (TLS) y opciones de autenticación de doble factor para cuentas profesionales.
- **Certificaciones**: Al ser una entidad de la UE, cumple con los estándares europeos de seguridad, aunque su enfoque "offshore" en el tratamiento de ciertos datos de la darknet implica que el usuario debe aplicar sus propias capas de seguridad al integrar la API.

Otros
Es relevante mencionar que IntelX aplica una política de "Neutralidad de Datos" agresiva. A diferencia de buscadores como Google, no desindexan contenido basándose en solicitudes de "derecho al olvido" de buscadores si consideran que el dato es parte de un registro histórico de una brecha, lo que obliga a la empresa española a ser muy cuidadosa con la trazabilidad de la información obtenida.

Fuentes consultada:
- Términos y condiciones de IntelX
- Política de privacidad
- Documentación técnica de la API
- Directrices de cumplimiento de Intelligence X