THREAT INTELLIGENCE DE LA DARK WEB

DarknetSearch

by Kaduu AG

Monitorización continua de la dark web, la deep web y la web abierta que le ayuda a encontrar
filtraciones, activos expuestos y suplantaciones antes de que los atacantes los usen.

VISIÓN GENERAL PARA CLIENTES · RECORRIDO POR EL PRODUCTO



darknetsearch.com

AGENDA

Qué veremos

1 **El desafío**

Por qué la exposición en la dark web es un riesgo creciente para toda organización

2 **Visión general de la plataforma**

Un panel para una visibilidad continua de las amenazas

3 **Funciones principales**

Búsqueda, exposición de credenciales, Darknet Chatter, superficie de ataque, protección de marca

4 **Alertas e informes**

Monitorización automatizada, incidentes e informes ejecutivos

5 **Pensado para su equipo**

Casos de uso para CISO, analistas de threat intelligence, SOC y MSSP

6 **Primeros pasos**

Prueba gratuita, informe del darknet y próximos pasos

EL DESAFÍO

Sus datos ya se están vendiendo donde usted no los ve

Credenciales robadas, logs de malware y dominios clonados circulan por mercados de la dark web, canales de Telegram, sitios de paste y foros criminales mucho antes de aparecer en un titular sobre una brecha.

24/7

Monitorización continua de fuentes de la dark web, la deep web y la web abierta

2200+

Canales de Telegram y foros de cibercrimen vigilados

10+

Factores de riesgo puntuados por organización, de forma automática

24 h

Plazo para un informe completo de exposición en el darknet

PRESENTAMOS DARKNETSEARCH

Una plataforma para la visibilidad de amenazas externas.

DarknetSearch analiza de forma continua la dark web, la deep web y la web abierta para que sepa siempre cuándo están expuestas sus credenciales, su infraestructura o su marca, y pueda actuar antes que los atacantes.

01

Detección de filtraciones

Identifique en tiempo real credenciales robadas, dispositivos comprometidos y exposición de la cadena de suministro.

02

Attack Surface Discovery

Vea su red como la ve un atacante: CVE, puertos abiertos y shadow IT.

03

Protección de dominios y marca

Detenga el phishing y el typosquatting antes de que los dominios clonados se activen.

LA PLATAFORMA DE UN VISTAZO

Su puntuación de riesgo, en un solo panel

Cada organización recibe una puntuación de riesgo global en tiempo real, calculada a partir del historial de filtraciones, la higiene de credenciales, los puertos expuestos y la exposición en buscadores, con una cronología de 12 meses para seguir la evolución.

— **Puntuación de riesgo global**: un único valor de 0 a 100 comparado con su sector y la competencia.

— **Principales factores de riesgo**: filtraciones recientes e históricas, contraseñas débiles, puertos abiertos inusuales, exposición en buscadores.

— **Cronología del riesgo**: evolución del riesgo de su organización y de su infraestructura durante el último año.

— **Estadísticas de credenciales y usuarios filtrados**: total de registros filtrados, stealer logs, combo lists y usuarios de mayor riesgo.



Puntuación de riesgo | Comparativa | Cronología de tendencia | Estadísticas de credenciales

FUNCIÓN PRINCIPAL · 01

Busque en la dark web y la deep web en segundos

Quick search recorre todas las fuentes de datos a la vez; Expert search permite a los analistas crear consultas booleanas precisas sobre una fuente concreta, ideal tanto para la primera respuesta como para la investigación en profundidad.

— **Busque por lo que quiera**: dominio, correo electrónico, nombre, IP, marca, contraseña, nombre de archivo o nombre de host.

— **14 fuentes especializadas**: filtraciones en bruto, credenciales filtradas y en bruto, Telegram, Discord, pastes y más.

— **Generador de consultas a medida**: combine los operadores AND / OR / NOT, rangos de fechas y tipos de archivo para mayor precisión.

— **Resultados inmediatos y sin duplicados**: credenciales, brokers, pastes y casos de phishing ordenados por relevancia.



Filtraciones en bruto | Telegram | Discord | Data brokers | Logs SSL

FUNCIÓN PRINCIPAL · 02

Exposición de credenciales, puntuada y priorizada

Cada par de usuario y contraseña filtrado vinculado a su dominio se deduplica y se puntúa, para que su equipo se centre en las cuentas que más importan y no en miles de filas en bruto.

— **Puntuaciones de novedad, riesgo y reutilización**: vea al instante qué credenciales son nuevas, de alto riesgo o reutilizadas en otros sitios.

— **Infraestructura propia frente a terceros**: separe los accesos internos de la exposición de socios y clientes.

— **Stealer logs y combo lists**: detecte credenciales robadas por malware, no solo volcados antiguos de brechas.

— **Informes comparativos**: compare la exposición de credenciales entre filiales, marcas o competidores.



Credenciales únicas | Reutilización de contraseñas | Stealer logs | Combo lists | Cuentas de dominio

FUNCIÓN CLAVE · 03

Monitorización en tiempo real de conversaciones del darknet

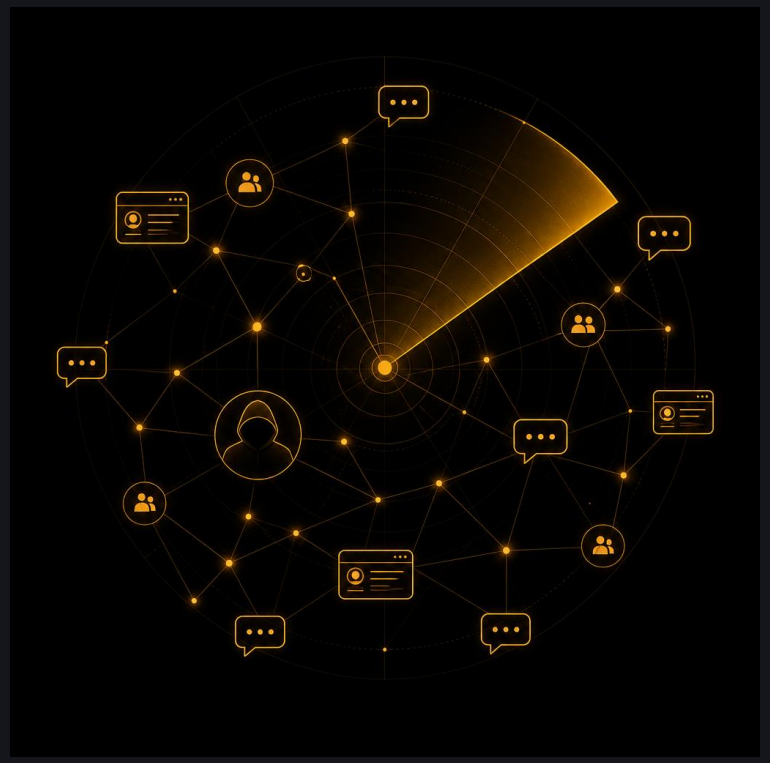
Siga las publicaciones de foros de cibercrimen, las ofertas de mercados y la actividad de actores de amenazas en cuanto aparecen, en miles de canales de Telegram, foros y sitios de carding.

— **Más de 2.200 canales monitorizados**: Telegram, Discord y foros oscuros, con búsqueda mediante operadores booleanos.

— **Seguimiento de actores de amenazas**: atribuya las conversaciones a alias conocidos y vigile directamente los grupos de ransomware.

— **Resultados categorizados**: mercados, filtraciones y datos, carding/fraude, hacking, servicios, debate.

— **Investigaciones en vivo**: consulte Tor / I2P y canales cerrados con discreción a través de nuestra red de proxies.



Mercados | Filtraciones y datos | Carding / fraude | Actores de amenazas | Búsqueda en vivo

FUNCIÓN CLAVE · 04

Análisis de superficie de ataque y exposición de código

Vea su organización como la ve un atacante. Descubra activos olvidados, configuraciones de riesgo y secretos filtrados en código público antes de que otros los encuentren.

— **Attack Surface Discovery**: visibilidad automática de hosts expuestos a internet, CVE y puertos abiertos.

— **Detección de shadow IT**: localice activos añadidos por desarrolladores, agencias o autónomos que desconocía.

— **Análisis de exposición de código**: búsquedas por palabras clave en GitHub, Gist, GitLab, Postman y Google dorking.

— **Delimitación por colaboradores**: cartografíe los repositorios públicos y colaboradores de una organización para afinar los análisis.



CVE · Puertos abiertos · GitHub · Gist · Postman

FUNCIÓN CLAVE · 05

Protección de dominio y de marca

Impida que los actores de amenazas suplanten su marca antes de que un sitio de phishing esté activo: dominios similares, tiendas de apps y redes sociales.

— **Detección de typosquatting**: monitorización diaria de nuevos registros de dominio y de los registros de transparencia SSL.

— **Análisis visual de suplantación de logotipos**: WHOIS, geolocalización, capturas de pantalla y puntuación de riesgo web de cada dominio hallado.

— **Monitorización de tiendas de apps y redes sociales**: apps falsas en iTunes / Google Play y perfiles falsos de la marca.

— **Informes de riesgo específicos**: informes de suplantación de dominios, VIP Executive, redes sociales y seguridad de aplicaciones.



Typosquatting | Transparencia SSL | Tiendas de apps | Informe VIP Executive

FUNCIÓN CLAVE · 06

Alertas automáticas y respuesta a incidentes

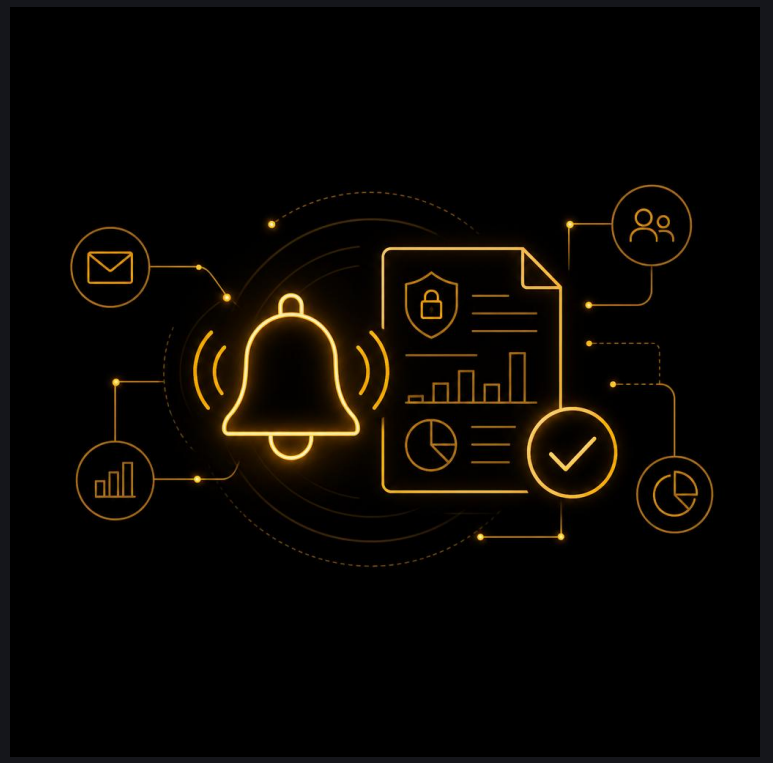
Convierta la monitorización continua en acción. Cree las reglas una vez y reciba un aviso en cuanto algo importe, con todo el contexto para investigar de inmediato.

— **Reglas de alerta personalizadas**: cree consultas sobre cualquier fuente de datos y elija la frecuencia de notificación.

— **Feed de incidentes**: cada activación registrada con estado, fuente y acceso con un clic a los datos en bruto.

— **Entidades extraídas**: dominios, nombres de usuario y contraseñas extraídos automáticamente de cada coincidencia.

— **Exclusiones inteligentes**: silencie falsos positivos y coincidencias recurrentes con reglas de exclusión reutilizables.



Reglas de alerta | Incidentes | Exclusiones | Webhooks

FUNCIÓN CLAVE · 07

Informes ejecutivos y comparativa sectorial

Convierta datos de amenazas en bruto en informes listos para el consejo, programados automáticamente o generados bajo demanda, y comparados con su sector y su competencia.

— **Evaluaciones completas**: informes con un clic sobre riesgo de brecha, infraestructura, suplantación y seguridad de apps.

— **Informe comparativo de credenciales filtradas**: compare la exposición entre divisiones, filiales o empresas del sector.

— **Envío programado**: los informes periódicos llegan solos a su bandeja de entrada, sin trabajo manual.

— **Darknet Exposure Report**: análisis único en profundidad en 24 horas, entregado en PDF + datos CSV en bruto.



Riesgo de brecha | Riesgo de infraestructura | Suplantación de dominios | VIP Executive | Informes programados

PENSADO PARA SU EQUIPO

Información específica para cada rol en ciberseguridad

CISO

Visibilidad estratégica y priorización del riesgo

Visibilidad continua de credenciales filtradas, accesos expuestos y brechas de terceros, traducida en información clara y lista para el consejo, para gobernanza y cumplimiento.

Analistas de threat intelligence

Detectar, correlacionar, contextualizar

Unifique la búsqueda en la dark web, la monitorización de datos robados, el análisis de stealer logs y el perfilado de actores de amenazas en un único flujo de trabajo para validar antes las amenazas emergentes.

Analistas de SOC

Respuesta más rápida y precisa

Enriquezca el SIEM y las investigaciones de incidentes con señales externas de la dark web para confirmar incidentes antes, reducir falsos positivos y acortar el tiempo medio de respuesta.

PREPARADO PARA EMPRESAS Y MSSP

Diseñado para escalar entre equipos, marcas y clientes

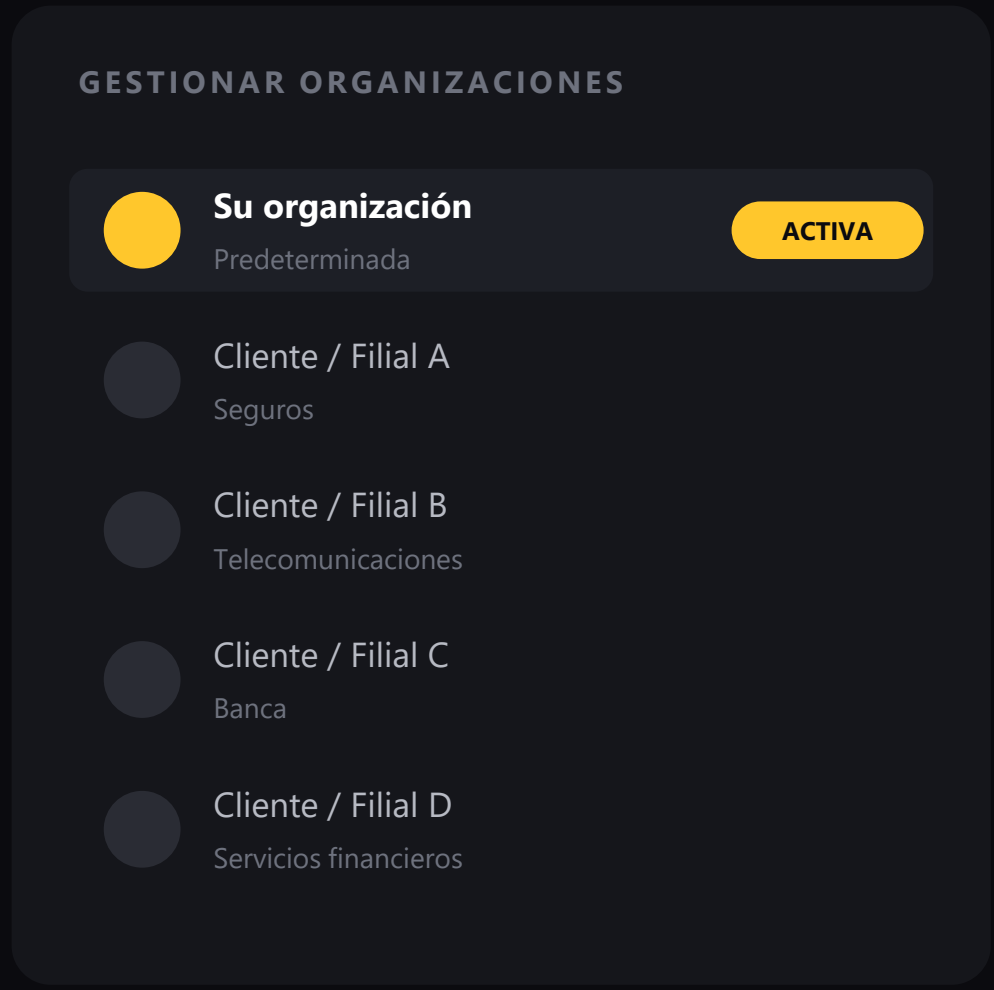
Gestione cada filial, marca o cliente desde una sola cuenta, con roles granulares, visibilidad del uso y acceso completo a la API para automatizar.

— **Gestión de organizaciones multiinquilino —** cambie entre cuentas de clientes al instante

— **Control de acceso basado en roles con 2FA —** administradores del sistema, usuarios de la organización y más

— **Paneles de uso —** controle la cuota por servicio (búsquedas, alertas, informes, llamadas a la API)

— **REST API completa —** envíe alertas y datos de filtraciones directamente a su SIEM o SOAR



POR QUÉ CONFÍAN EN NOSOTROS

Equipos de seguridad de distintos sectores confían en nosotros

"

Usa DarknetSearch para detectar en tiempo real filtraciones de datos de clientes, activos expuestos y suplantación de dominios. Las alertas y los informes por API ayudan a su SOC a responder más rápido.

Cloud y Olé

Proveedor de seguridad gestionada

"

Detecta credenciales filtradas y brechas de datos en la dark web y envía las alertas directamente a su SIEM para rotar credenciales de forma proactiva a escala empresarial.

Bühler

Fabricante industrial global

"

Monitoriza la dark web en busca de filtraciones y datos expuestos que afectan a las ONG a las que presta apoyo; valora su facilidad de uso y la relevancia de la inteligencia pese a los recursos limitados.

CyberPeace Institute

ONG suiza de ciberseguridad

Valorado en G2 · g2.com/products/kaduu/reviews

PRIMEROS PASOS

Vea su exposición. Empiece hoy.

Prueba gratuita de 7 días

Explore la plataforma DarknetSearch completa, sin compromiso y sin tarjeta de crédito.

EMPEZAR PRUEBA GRATUITA

Informe de exposición en la darknet

Análisis puntual en profundidad: credenciales expuestas, tendencias de filtraciones, usuarios de riesgo y dominios suplantados. Entrega en PDF + CSV en 24 horas.

SOLICITAR SU INFORME

Oferta a medida

Obtenga un presupuesto para empresas o MSSP ajustado al tamaño y al perfil de riesgo de su organización.

SOLICITAR PRESUPUESTO



Descubramos qué ya está expuesto.

Gracias: estaremos encantados de mostrarle la puntuación de riesgo en vivo de su organización.

---

darknetsearch.com

Kaduu AG · Suiza

