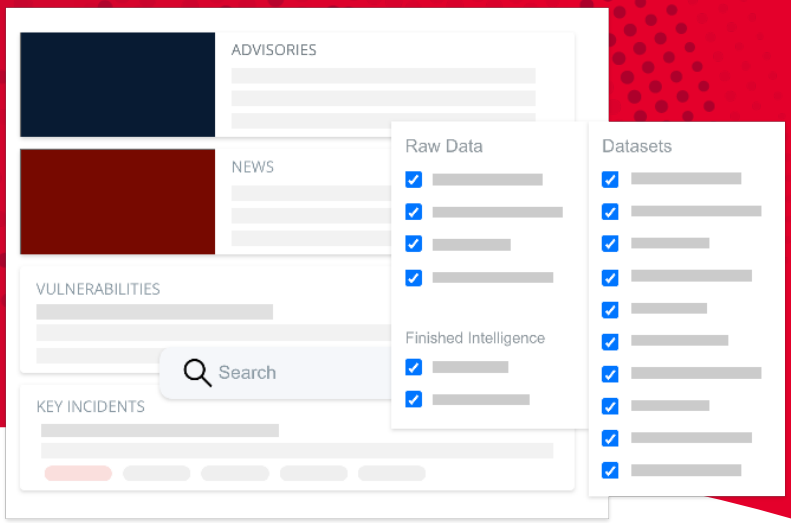
ZEROFOX

FICHA TÉCNICA

Módulo de búsqueda de amenazas

Funciones de acceso, búsqueda e investigación con nuestra inigualable inteligencia sobre amenazas externas, filtrada por los expertos en amenazas de ZeroFox



Reto

Las amenazas externass prosiguen su evolución en la superficie de ataque pública, así que, ahora más que nunca es imperativo contar con inteligencia organizada por expertos. Extraer ideas y correlacionar datos dispares es fundamental para cumplir con los requisitos de recopilación de inteligencia. Sin embargo, cuando hablamos de búsqueda de amenazas, muchas organizaciones carecen de la visibilidad y el contexto necesarios para encajar todas las piezas.

Para poder adelantarse a las últimas ciberamenazas, navegar por el inmenso océano de amenazas digitales actuales y hacer recomendaciones de seguridad fundamentadas, los investigadores necesitan contar con acceso directo y sin restricciones a todo el espectro de inteligencia de amenazas relevante para las operaciones y el sector de cada organización.

Solución

El módulo de búsqueda de amenazas de ZeroFox (integrado en la plataforma de ZeroFox) proporciona una interfaz con la que realizar búsquedas en el vasto lago de datos sobre inteligencia de amenazas de ZeroFox, que incluye información sobre ataques e indicadores de compromiso. Las funciones de búsqueda de amenazas externas de ZeroFox suplen las lagunas de inteligencia concediendo a los responsables de dar respuesta a incidentes, los analistas y los investigadores acceso ilimitado y con capacidad de búsqueda a petabytes de inteligencia procesada, conjuntos de datos y datos brutos que se recopilan y filtran de forma global según los requisitos de inteligencia del cliente.

CARACTERÍSTICAS CLAVE

- **Búsquedas en una enorme base de datos** de inteligencia procesada, conjuntos de datos y datos brutos almacenados en el lago de datos de amenazas de ZeroFox
- **Acceso directo** a incidentes, noticias, avisos, vulnerabilidades, exploits, dominios C2, credenciales comprometidas, direcciones IP y tarjetas de crédito robadas, comunicaciones de canales encubiertos, etc.
- **Contexto adicional procedente de las conclusiones obtenidas por los analistas**, como la atribución del delito al ciberdelincuente, los detalles de TTP, CVE y gravedad de la campaña, así como recomendaciones

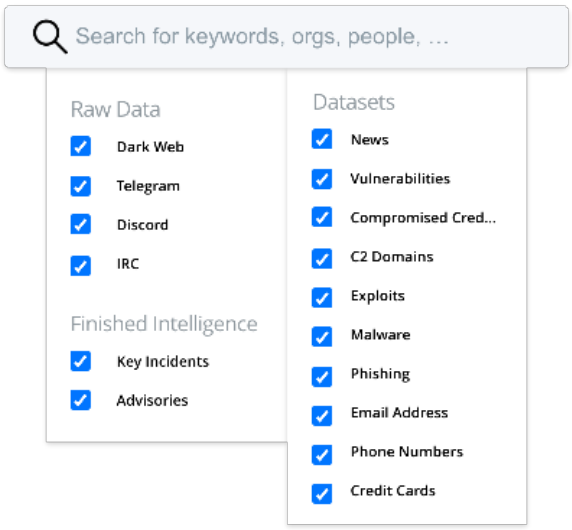
VENTAJAS

- **Permite realizar investigaciones fácilmente** para obtener más visibilidad sobre el panorama de amenazas concreto de su organización
- **Aprovecha la recopilación y correlación de datos de amenazas diferentes** desde un prisma único y global en la propia plataforma
- **Facilita la búsqueda de amenazas proactiva** para desvelar posibles actividades maliciosas y ataques ocultos basados en TTP o en indicadores de compromiso o ataque conocidos
- **Permite buscar, filtrar y extraer de forma granular y rápidamente información** a partir de petabytes de datos de inteligencia única sobre amenazas

FICHA TÉCNICA

Inigualable inteligencia externa con capacidad de búsqueda, para la investigación de incidentes y la búsqueda de amenazas

El módulo de búsqueda de amenazas de ZeroFox proporciona al personal encargado de dar respuesta a incidentes, y a analistas y cazadores de amenazas acceso a información filtrada, global y sin procesar, a través de una búsqueda unificada para potenciar sus investigaciones. Realice búsquedas en inteligencia recopilada de la web oscura y de fuentes de datos encubiertas, incluida la inteligencia humana (o HUMINT) operativa oscura. Identifique exposiciones críticas y obtenga una alerta temprana si se detectan planificaciones de ataques y conversaciones relacionadas. Pivotee rápidamente a partir de la inteligencia correlacionada y recopile más evidencias de una enorme colección de datos de amenazas sin procesar. Además, aproveche las últimas noticias sobre ciberseguridad, los avisos de los analistas, las investigaciones sobre amenazas y los informes sobre vulnerabilidades.



Busque entre varios tipos de datos y conjuntos de datos brutos sobre amenazas mediante consultas avanzadas para identificar las conclusiones y acotar las investigaciones.

Fuente de datos	Descripción	Campos de búsqueda
Web oscura	Datos de la web profunda y la web oscura que incluyen conversaciones sobre ciberataques, intercambio de paquetes de violaciones de seguridad y menciones de su marca que los ciberdelincuentes pueden aprovechar para perjudicar a su organización, sus empleados o a otros implicados.	text body
Telegram	Un amplia recopilación de comunicaciones y chats encubiertos pertinentes, procedentes de mensajes cifrados de Telegram.	channel_name, first_name, last_name, message, user
Discord	Un conjunto de mensajes de Discord procedentes de los canales.	author.username, channel_name, content, server_name
IRC	Mensajes comunicados a través de Internet Relay Chat que incluyen canales donde se producen ciberataques y actividad maliciosa.	channel, message, sender
Credenciales comprometidas	Una serie de credenciales que se han enviado a personas no autorizadas y que se pueden utilizar para acceder a información sin autorización.	username, password, email, dumpname, impacted_domain.text, source
Dominios C2	Dominios que aparecen en infraestructuras y configuraciones de mando y control (C2) de malware.	domain, triage_tags
Exploits	Scripts de exploits que generan los investigadores de seguridad y los ciberdelincuentes para aprovechar recursos vulnerables.	title, author, sources, code
Malware	Malware reciente y metadatos relevantes, como familia y hashes.	md5, sha1, sha256, sha512, family, tags
Phishing	Una lista de URL que se han utilizado para perpetrar ataques de phishing.	domain, url, cert.authority
Direcciones de correo electrónico	Direcciones de correo electrónico que se han utilizado para lanzar un ciberataque. Pueden haber sido secuestradas por un ciberdelincuente o utilizadas como infraestructura zombi.	email, domain, tags
Números de teléfono	Una lista de números de teléfono utilizados por los ciberdelincuentes para cometer estafas mediante, por ejemplo, smishing.	phonenumber, tags
Tarjetas de crédito	Tarjetas de crédito comprometidas que se han descubierto en data dumps.	cc_bin, cc_num, dumpname

¿LE GUSTARÍA COMPROBARLO USTED MISMO?

Solicite una demostración
Regístrese en zerofox.com/request-a-demo/

Más información
Visite zerofox.com
Contacte con nosotros: sales@zerofox.com /
+1 855 736 1400

ACERCA DE ZEROFOX

ZeroFox proporciona a las empresas protección, inteligencia y medidas para frustrar las amenazas contra marcas, individuos, recursos y datos en toda la superficie de ataque pública. ZeroFox combina IA avanzada y servicios expertos de inteligencia humana para detectar y analizar amenazas complejas y dirigidas, y servicios de disrupción automatizados para neutralizar la infraestructura de los atacantes.

ZEROFOX