Servicio integral
de protección contra
riesgos digitales

Kaspersky Digital Footprint Intelligence

kaspersky bring on the future

Preguntas para expertos

¿Cuál es la mejor manera de iniciar un ataque contra su empresa?

¿Cuál es la forma más rentable de atacarlo?

¿Qué información está disponible para los atacantes que eligieron su empresa como objetivo?

¿Su infraestructura ya está comprometida y no lo sabe?

Kaspersky Digital Footprint Intelligence responde a estas y otras preguntas, ya que nuestros expertos crean una imagen integral de su estado de ataque, identifican puntos débiles ideales para ser aprovechados y revelan pruebas de ataques pasados, presentes e incluso planificados..

Introducción

A medida que su negocio crece, la complejidad y la distribución de sus entornos de TI también lo hacen, lo que plantea el desafío de proteger una presencia digital ampliamente distribuida sin control ni propiedad directa. Los ambientes dinámicos e interconectados permiten que las empresas obtengan grandes beneficios. Sin embargo, el constante aumento de la interconectividad también está ampliando el área de ataque. Dado que los atacantes son cada vez más hábiles, es vital no solo disponer de una imagen precisa de la presencia en línea de su organización, sino también poder llevar un seguimiento de sus cambios y reaccionar ante amenazas externas dirigidas a los activos digitales expuestos.

Si bien las organizaciones utilizan una amplia gama de herramientas en sus operaciones de seguridad, sigue habiendo amenazas digitales al acecho que requieren capacidades muy específicas, como detectar y mitigar filtraciones de datos, monitorear planes y esquemas de ataque de ciberdelincuentes ubicados en foros de la web oscura, entre otras. Para ayudar a los analistas de seguridad a explorar la visión que tiene el adversario de los recursos de su empresa, detectar rápidamente los posibles vectores de ataque disponibles para ellos y ajustar sus defensas en consecuencia, Kaspersky creó Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence proporciona lo siguiente:

Kaspersky Digital Footprint Intelligence es un servicio integral de protección contra riesgos digitales que ayuda a los clientes a supervisar sus activos digitales y detectar amenazas desde la web superficial, profunda y oscura.

Reconocimiento de redes

Identificación de los recursos de red del cliente y los servicios expuestos que son un potencial punto de entrada para un ataque. Análisis personalizado de vulnerabilidades existentes, con una evaluación integral de riesgos basada en la puntuación base del CVSS, la disponibilidad de exploits públicos, la experiencia de pruebas de penetración y la ubicación del recurso de red (alojamiento/infraestructura).

Supervisión de la web oscura

Monitoreo constante de decenas de recursos de la web oscura (foros, ransomware, blogs, sistemas de mensajería, sitios de tor, etc.), que detecta todas las referencias y amenazas relacionadas con su empresa, clientes y partners. Análisis de ataques selectivos activos o que se estén planificando, campañas de APT dirigidas a su empresa, sector y regiones de operaciones.

Descubrimiento de filtraciones de datos

Detección de credenciales, tarjetas bancarias, números de teléfono y otra información confidencial de empleados, clientes y partners en riesgo, que se puede usar para realizar un ataque o que significa un riesgo para la reputación de la empresa.

Detección de amenazas

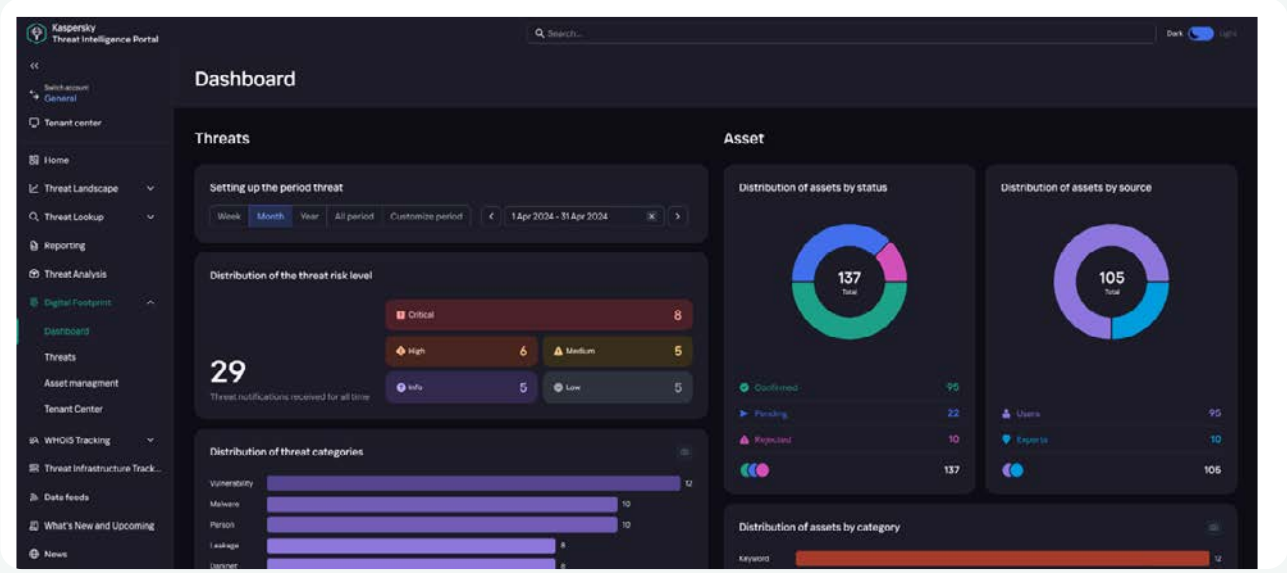
Supervisión de actividades fraudulentas que pueden dañar la reputación de una empresa o engañar a los clientes.

Funcionamiento

Configurar	Recopilar	Filtro	Reacción
Descubrimiento de la información sobre los activos digitales de la empresa	Recopilación automatizada de datos desde la web superficial, profunda y oscura, así como de la base de datos de Kaspersky	Detección de amenazas, análisis y priorización administrada por analistas	Envío de notificaciones sobre amenazas operativas en Kaspersky Threat Intelligence Portal o a través de la API

Resultados clave del servicio

1. Alertas sobre amenazas en Threat Intelligence Portal
2. Cuota de búsqueda en la base de datos de la red oscura
3. Cuota de búsqueda en la base de datos de las redes sociales
4. Presentaciones y sesiones de preguntas y respuestas con expertos
5. Datos legibles por máquina
6. Informes analíticos elaborados por nuestros especialistas
7. Solicitudes de ataque



Tipos de amenazas

Kaspersky Digital Footprint Intelligence permite a las organizaciones responder de forma rápida y eficaz ante posibles amenazas mediante alertas en tiempo real. Esto reduce la probabilidad de dañar la reputación de la marca, la confianza de los clientes y las operaciones empresariales en general. Las empresas pueden personalizar las capacidades de supervisión del servicio para satisfacer sus necesidades específicas, mientras que los informes y análisis integrales ofrecen información valiosa sobre el alcance y el impacto del uso no autorizado de la marca y otros riesgos potenciales.

Amenazas relacionadas con el perímetro de red

- Servicios de red mal configurados
- Identificación de las vulnerabilidades
- Recursos desfigurados o comprometidos

Amenazas relacionadas con la web oscura

- Estratagemas de fraude y planes de los ciberdelincuentes
- Venta y filtración de datos
- Actividades de informantes internos

Amenazas relacionadas con el malware

- Ataques de phishing
- Ataques selectivos
- Campañas de APT

Filtraciones de datos

- Recursos corporativos en riesgo
- Tarjetas de crédito en riesgo
- Credenciales comprometidas

Fuentes de inteligencia

Es esencial que nuestros clientes tengan una comprensión integral de su postura de seguridad externa. Para brindar esta información, los analistas de seguridad de Kaspersky recopilan y agregan información de las siguientes fuentes de inteligencia:

Sus datos no estructurados

- Direcciones IP
- Dominios de la empresa
- Marcas comerciales
- Palabras clave
- Rangos de red
- Números de tarjetas BIN/IIN
- Información de empleados

Inventario del perímetro de la red

Web superficial, profunda y oscura

Base de conocimientos de Kaspersky

Alertas de amenazas

Solicitudes de ataque

Búsqueda en tiempo real en las fuentes de Kaspersky y la red superficial y oscura

Informes analíticos

Servicio complementario

Valores comerciales

Kaspersky Digital Footprint Intelligence ofrece potentes beneficios y un valor significativo a su organización:

Proteja su marca

Detecte amenazas potenciales en tiempo real para proteger la reputación de su marca, preservar la confianza de sus clientes y reducir el riesgo de pérdidas financieras y daños en las operaciones empresariales.

Reduzca los ciberriesgos

Brinde a las partes interesadas (director de experiencia de cliente y Junta Directiva) información sobre dónde ubicar el gasto en ciberseguridad, lo que revelará las brechas de la configuración actual y los riesgos que acarrean.

Reaccione más rápido

El contexto adicional de las alertas de seguridad mejora la respuesta ante incidentes y reduce su tiempo medio de respuesta (MTTR).

Disminuya la superficie de ataque

Gestione la presencia digital de su empresa y controle los recursos de red externos para minimizar los vectores de ataque y las vulnerabilidades que pueden usarse en un ataque.

Comprenda a sus adversarios

Más vale prevenir que curar: sepa lo que los ciberdelincuentes planean y hablan sobre su empresa en la red oscura para que la empresa esté preparada.

Conozca lo desconocido

Mejore su capacidad de resistencia ante ciberataques e identifique las amenazas externas a la jurisdicción de sus equipos de seguridad internos.

Para obtener más información sobre los distintos planes de suscripción, comuníquese con nuestro equipo.

Comuníquese con nosotros

Kaspersky Digital Footprint Intelligence

Más información

latam.kaspersky.com

© 2024 AO Kaspersky Lab.
Las marcas comerciales registradas y las marcas de servicio pertenecen a sus respectivos propietarios.

#kaspersky
#bringonthefuture