Fraudes Digitales

Detecte y neutralice fraudes que personifican su empresa

La plataforma Axur ofrece monitoreo automatizado, inspección mejorada mediante IA y eliminación de ultra presición para neutralizar vectores de ataque externos.

Problema

Los ciberdelincuentes explotan técnicas sofisticadas para personificar su marca en varios vectores: ya sea a través de campañas de phishing, perfiles falsos, malware disfrazado o nombres de dominio que se asemejan mucho al original. Los equipos de seguridad se ven desafiados por la creciente prevalencia de estas amenazas persistentes, agotando los recursos y prolongando los tiempos de respuesta. Estos riesgos socavan la confianza y la lealtad del cliente, y las fraudes digitales no solo erosionan la integridad de la marca, sino que también aumentan los costos operativos como los contracargos.

Solución

La plataforma Axur alivia las cargas operativas al identificar y eliminar fraudes digitales que personifican su marca. Nuestra inspección avanzada basada en IA examina señales avanzadas como similitudes de logotipos e inicia automáticamente flujos de eliminación, sin necesidad de esperar una acción humana. Al reducir drásticamente el tiempo medio de contención (MTTC) y configurar conjuntos de reglas de automatización personalizadas, Axur fortalece sus defensas, asegurando una postura de ciberseguridad resiliente, simplificada y proactiva.

Phishing

La plataforma Axur detecta un intento de phishing y activa automáticamente la eliminación en solo 5 minutos, el tiempo de respuesta más rápido del mercado.

Con nuestra tecnología OnePixel única, la cobertura aumenta hasta un 52%.

Uso fraudulento de marca

Identifique el uso fraudulento del nombre de su empresa, asegurando protección contra asociaciones indebidas que puedan engañar o confundir a sus clientes.

Perfil falso en red social

Nuestra plataforma implementa modelos predictivos para identificar rápidamente el uso no autorizado del nombre de su marca y activos visuales, como logotipos y mascotas, en las principales redes sociales. Eliminaciones automáticas con notificaciones en 3 minutos.

El monitoreo incluye plataformas:

Malware

Monitoree la propagación del malware Trojan Banker y proteja a sus consumidores del robo de datos para transacciones financieras y compras fraudulentas. Los datos pueden contener los detalles del servidor C&C (Command and Control) de la máquina infectada.

Nombre de dominio similar

Inspeccione nuevos registros de dominios relacionados con su marca y manténgalos bajo vigilancia. Será el primero en saber si estos dominios alojan campañas de phishing o registran actividades sospechosas.

Uso de marca en búsqueda paga

Evite que competidores y estafadores aprovechen su marca en los principales anuncios pagos de los motores de búsqueda, como Google.

Aplicaciones móviles falsas

Obtenga visibilidad completa de las tiendas oficiales y sitios web de aplicaciones para rastrear aplicaciones falsas que se hacen pasar por su marca o representan algún riesgo para sus consumidores.

El mejor Takedown del mundo. Y podemos probarlo.

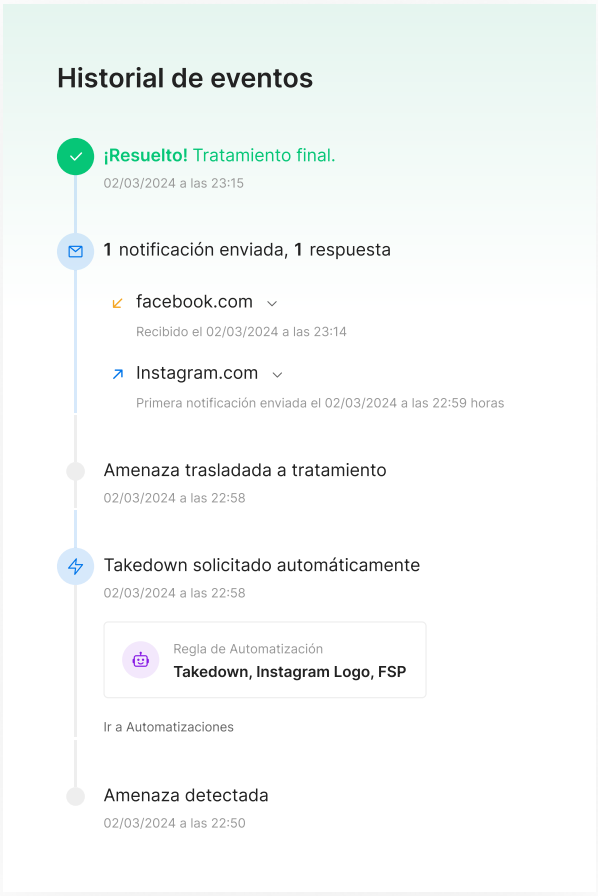
5 minutos
Para la primera notificación en casos de phishing y hasta 30 minutos para todos los demás incidentes.

98.9% tasa de éxito
Con la garantía de una nueva eliminación gratuita si el contenido vuelve a estar en línea dentro de los 15 días.

9h de uptime
Tiempo mediano para la eliminación de contenido con los takedowns de Axur.

Active Takedowns con flujos automáticos

Cada segundo cuenta para mitigar una amenaza. No es necesario esperar una intervención humana cuando más necesita acción. En 2023, el 86% de las detecciones de Axur se manejaron sin intervención humana.



Inspección y eliminación impulsadas por IA

La plataforma Axur analiza profundamente las señales para categorizar y priorizar amenazas. Al potenciar la automatización de takedowns, las acciones son rápidas y precisas, minimizando la exposición y fortaleciendo la resiliencia cibernética.

Principales atributos de la inspección

- 89 Puntuación de riesgo
- Similitud del logotipo de la marca
- Idioma del contenido
- Desambiguación del nombre de la marca
- Reconocimiento facial VIP
- Presencia de campos de contraseña
- ¡Y varios más!

Mantenga la vigilancia con Re-up

El takedown de Axur no se limita a la remediación inicial, sino que es un compromiso para garantizar que las amenazas contra su negocio permanezcan neutralizadas. Si algún contenido eliminado reaparece dentro de un período de 15 días, se detectará de inmediato y se tratará como un nuevo incidente, sin costo adicional para usted.

Maximice la defensa con Websafe Reporting

Axur colabora con principales entidades de ciberseguridad para reducir el alcance de contenido malicioso, disminuyendo el tiempo de exposición a fraudes. Estamos integrados con más de 30 organizaciones líderes en ciberseguridad.

Compilación de evidencia sin esfuerzo

Permita que la automatización simplifique la recolección de evidencia, desde copias HTML y capturas de pantalla hasta datos de dominio, ayudando en la toma de decisiones.

Vea todo esto en acción.

Conozca todas nuestras soluciones: axur.com

Agende una demo

///AXUR