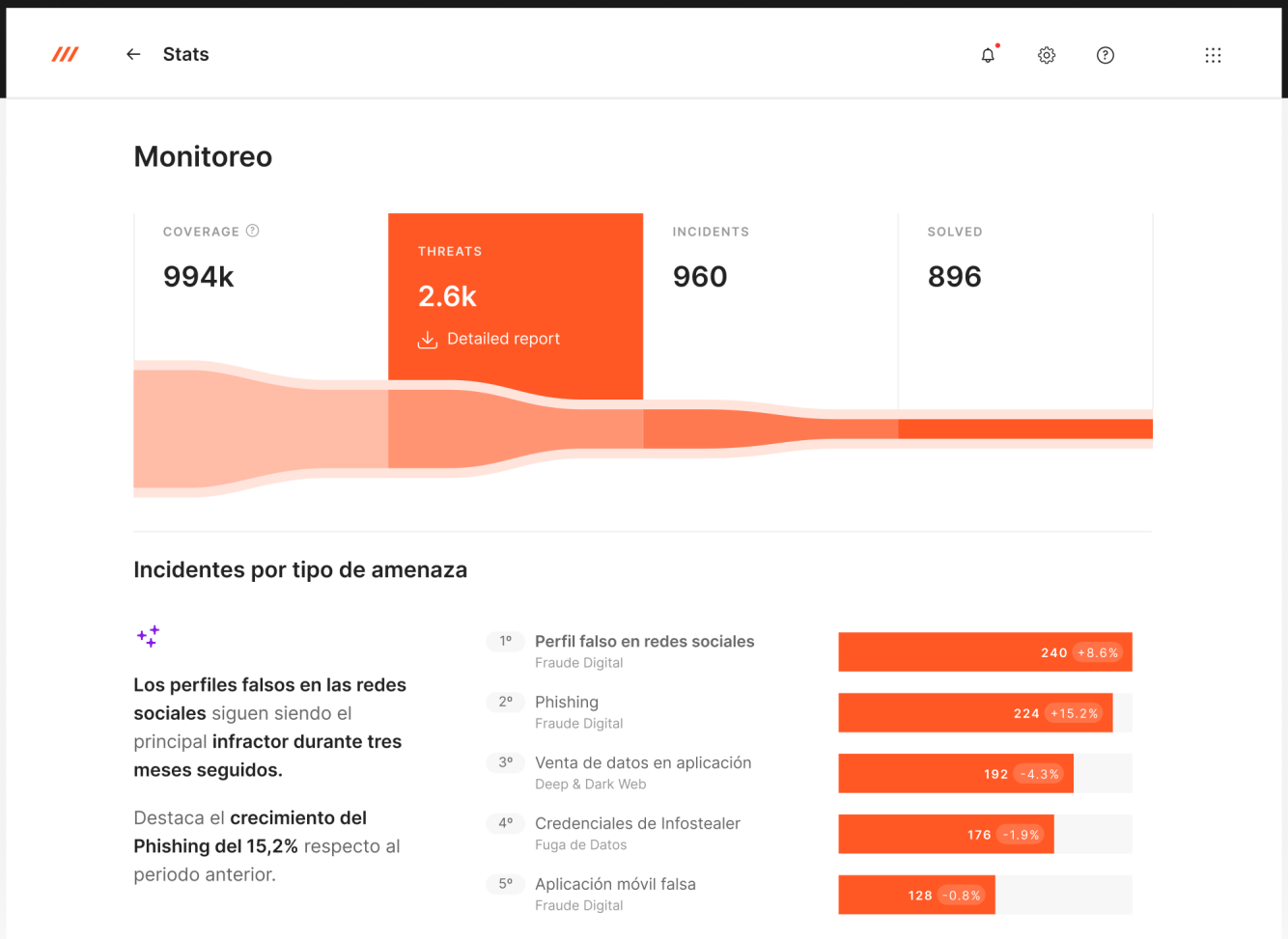
AXUR

Ciberseguridad Externa

Axur asume el trabajo pesado contra amenazas externas para que usted pueda ser el activo estratégico que su empresa necesita



Con un aumento del 75% en los ataques cibernéticos, necesita una plataforma de ciberseguridad externa avanzada que se destaque por ofrecer identificación y neutralización rápida de amenazas, flujos de trabajo de eliminación únicos en la industria e inteligencia integral sobre fraudes, ayudando a las empresas a contrarrestar amenazas digitales en evolución.

- Impulsado por inspección de IA
- Takedown con flujos automatizados
- Minimiza la ventana de ataque

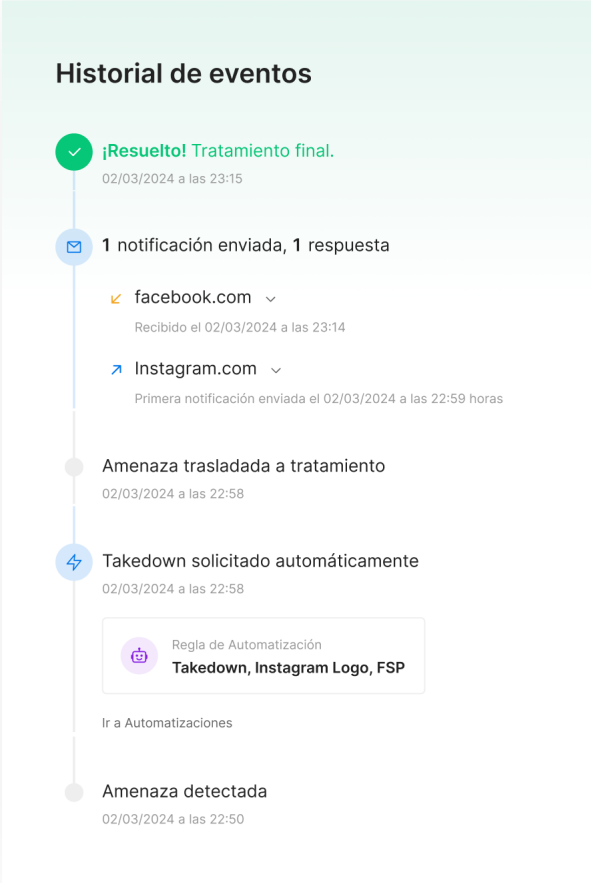
La inspección potenciada por IA es un cambio de juego contra el cibercrimen

Escale el análisis de señales masivas, buscando atributos clave para categorizar, priorizar y abordar de forma autónoma detecciones, ya sea para descartar falsos positivos o gestionar incidentes genuinos.

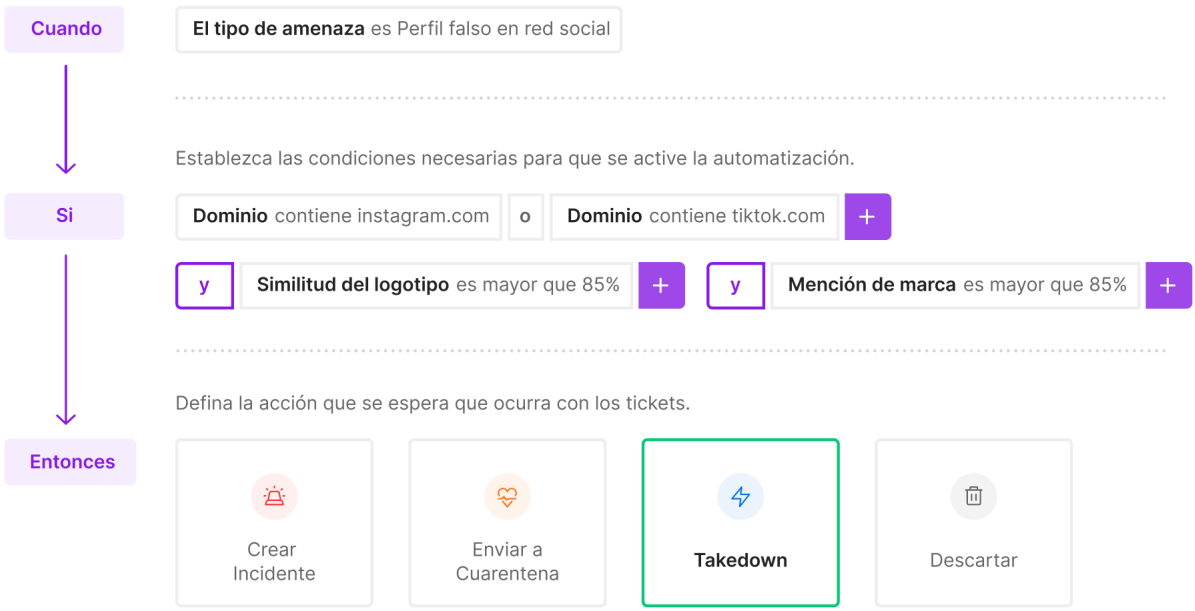
Algunos atributos inspeccionados que mejoran exponencialmente su gestión de amenazas incluyen:

- **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!

Más del 86% de las detecciones se gestionan sin contacto humano



Ejemplo real de resultados de una empresa del sector financiero.



Reglas de Automatización

Configure flujos de trabajo automatizados para utilizar un arsenal sin comparación operando 24×7 para su organización, identificando riesgos e iniciando solicitudes de remoción automáticas. Descanse tranquilo, sabiendo que las amenazas se abordan inmediatamente siempre que se cumplan sus condiciones especificadas.

///AXUR

Estándar oro para nuestro Takedown: eficiencia sin igual.

5 minutos
Mediana de tiempo para la primera notificación

98.9% tasa de éxito
Nuevo derribo gratis si el contenido reaparece en 15 días

9 horas de uptime
Mediana de tiempo para la resolución

Ejemplo real de resultados de una empresa del sector de Venta al por menor y Comercio electrónico durante un período de 1 mes.

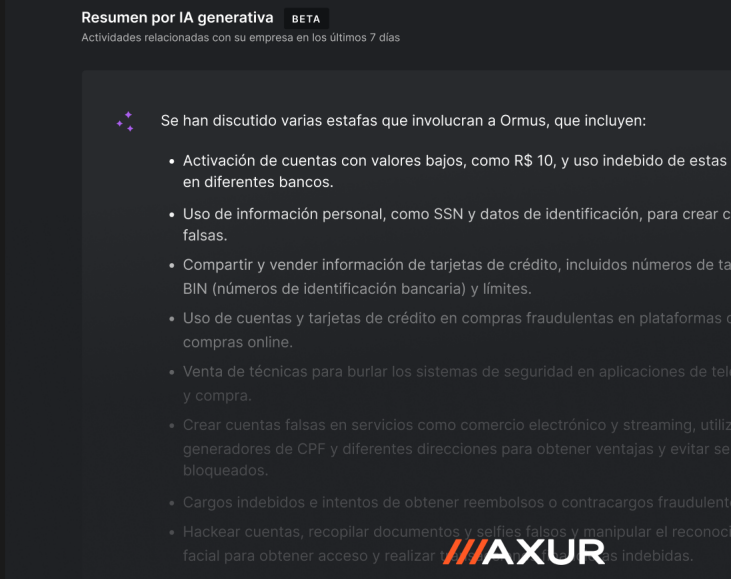
Takedowns automatizados, porque no puede esperar por la acción humana cuando necesita respuestas más rápidas.

Reduzca drásticamente el Tiempo Medio para Contener (MTTC), automatizando la parte del proceso que puede controlar con las notificaciones más rápidas y precisas del mercado. Optimize el análisis del proveedor con notificaciones orquestadas para el mejor camino y mensaje, desarrolladas con años de experiencia - y mejorando constantemente. Si la entidad notificada retrasa la respuesta, se activan automáticamente nuevos flujos para acelerar el Takedown por otra ruta. Todo esto permite la escalabilidad de las eliminaciones de forma ilimitada.

Inteligencia contra fraude para proteger su negocio

Comience su día con DeepChat, nuestro modelo generativo de IA que proporciona un informe sobre las menciones más relevantes de su marca en la Deep & Dark Web. Mejore su seguridad con alertas de anomalías en tiempo real, incluyendo menciones de la marca por encima de lo normal y seguimiento específico de palabras clave, asegurando atención inmediata a potenciales amenazas como ataques planificados o explotación de bugs.

- Resumen de IA Generativa
- Alertas de Anomalías
- Perfil de Actor de Amenazas



Soluciones avanzadas para proteger su negocio en el mundo digital

Fraudes digitales

Monitoree y detecte contenidos que se hacen pasar por su marca, con cobertura 24/7. Utilice el takedown más eficiente del mundo para eliminar automáticamente vectores de riesgo externos.

- Phishing
- Uso fraudulento de marca
- Malware
- Perfil falso en red social
- Aplicación móvil falsa
- Nombre de dominio similar
- Uso de marca en búsqueda paga

Fuga de datos

Detecte exposiciones de datos en tiempo real para proteger su superficie de ataque y mitigar riesgos.

- Credenciales de infostealer
- Exposición de tarjeta de crédito - para aplicaciones
- Exposición de tarjeta de crédito - para emisores
- Exposición de credencial corporativa
- Other sensitive data
- Exposición de código secreto
- Exposición de base de datos

Piratería Online

Recupere su ingreso que se está perdiendo en piratería y ventas irregulares.

- Producto falso o venta irregular
- Piratería de contenido

Deep & Dark Web

Supervise las amenazas y detecte menciones de su empresa en canales y grupos de la Deep & Dark Web. Realice un seguimiento de las menciones de marca, las palabras clave y el contenido multimedia.

- Busque cualquier término en miles de canales y grupos usando Explorar
- Alertas de anomalías

Ejecutivos y personas VIP

Monitoree la exposición de datos de las cuentas más sensibles de su empresa y reduzca el riesgo de spear phishing, ransomware y ataques que utilizan ingeniería social.

- Perfil falso en red social
- Exposición de información personal, credenciales, teléfonos o tarjetas de crédito

Threat Hunting

★ ¡Últimas noticias!

Mejore sus investigaciones de amenazas aprovechando una de las bases de datos de amenazas más grandes del mundo para analizar en profundidad y descubrir actividades sospechosas.

- Busque en la extensa base de datos de Axur con más de 23 mil millones de credenciales, así como URL y dominios
- Aprenda de incidentes pasados para prevenir ataques futuros y crear una estrategia de seguridad más resistente

Calificación de Seguridad

Evalúe y fortalezca su postura de seguridad eliminando riesgos externos y de terceros.

Agende su demo ahora

AGENDE UNA DEMO

Conozca todas nuestras soluciones: axur.com

Los líderes del mercado confían en nosotros

Domino's · Carrefour · Grupo Salinas Desde 1906 · Volkswagen · Gerdau Corsa · Haitong · Toyota · natura

bsi ISO/IEC 27001 Information Security Management Certified

///AXUR