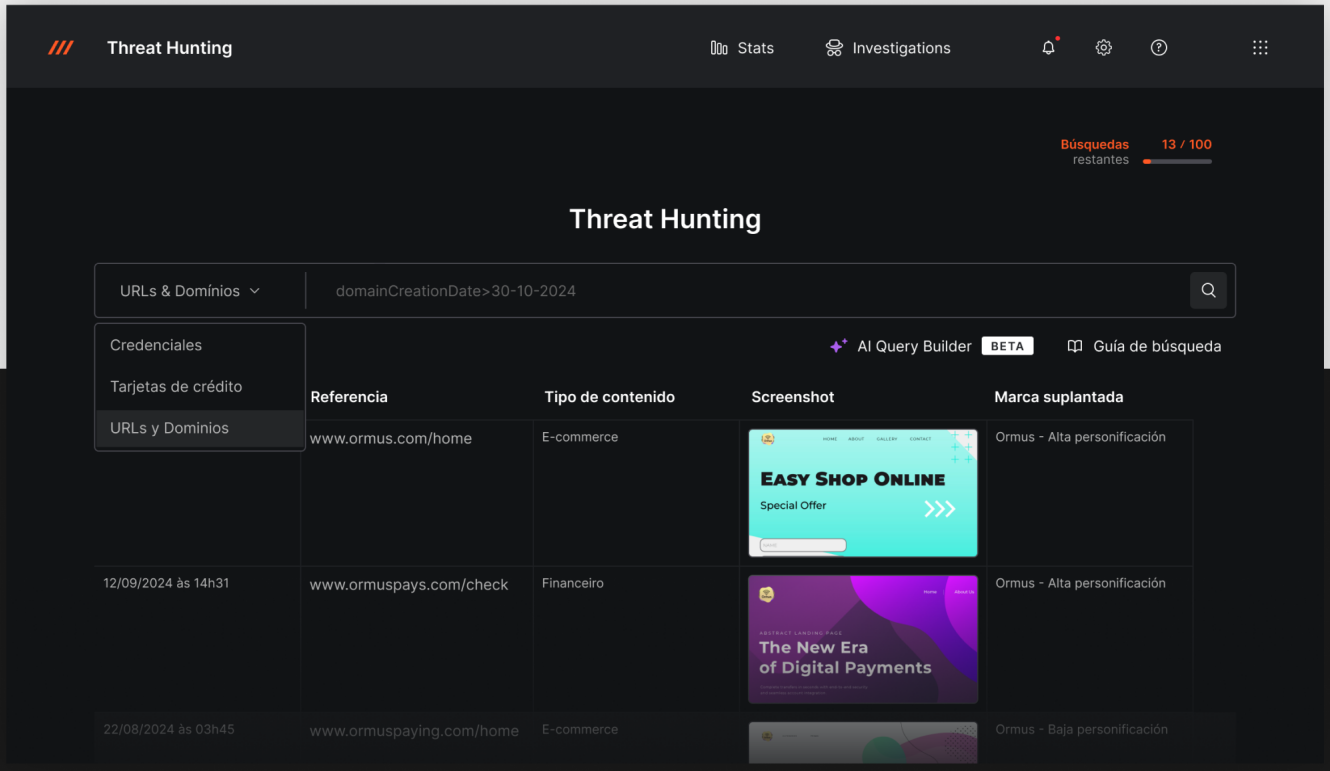
Threat Hunting - Phishing & Domain Intelligence

Haz hunting con el mayor banco de datos de URLs maliciosas, enriquecido por inteligencia artificial

Derribe cada amenaza con el mejor Takedown ⚡

Asegúrese de que ninguna amenaza pase desapercibida con la base de datos más grande enriquecida con IA para URLs maliciosas. Luego, aproveche las capacidades de eliminación más eficientes del mundo para remediar rápidamente cada una, brindando una protección inigualable.



Datos ficticios con fines comerciales

El Threat Hunting le permite explorar la amplia base de datos de Axur, realizando búsquedas detalladas de credenciales, tarjetas, archivos filtrados, URLs y dominios.

- Caza proactiva para investigar y detener el phishing de manera anticipada.
- Investigación de tendencias para rastrear ataques en su sector o entre sus competidores.
- Investigaciones de terceros para evaluar la seguridad de proveedores y socios.

Los estafadores están cada vez más inteligentes y difíciles de atrapar

El 70% de los sitios de phishing no usan nombres de marcas en los dominios, y el 18% ni siquiera los mencionan en el texto. La plataforma de Axur detecta cada una de estas amenazas sofisticadas, y va más allá de palabras clave para brindar una protección completa.

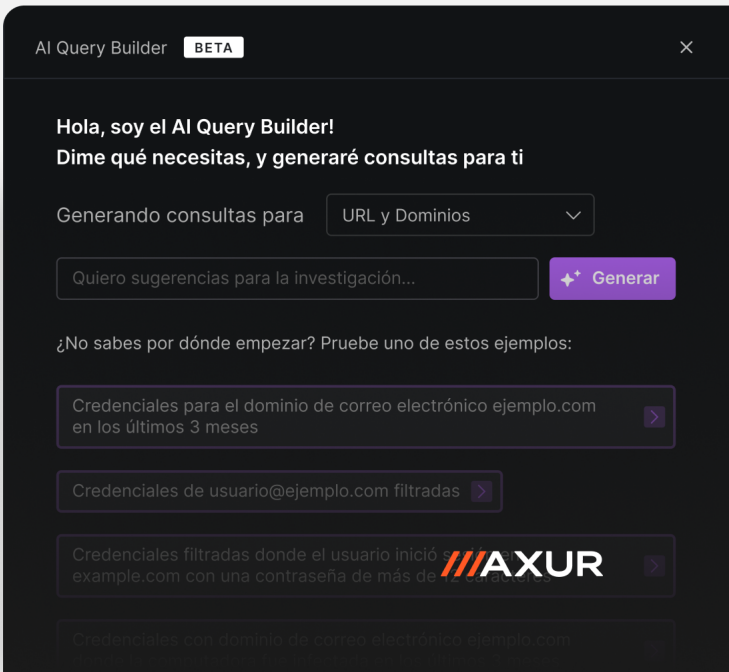
Un enfoque completamente nuevo para la protección de marcas

Agregamos 15 millones de nuevos sitios web a nuestro data lake todos los días. Y utilizamos nuestros modelos GenAI para inspeccionar y enriquecer cada señal.

Ultice la IA para crear consultas sin esfuerzo, haciendo sus investigaciones rápidas y fáciles

ElasticSearch/ OpenSearch

Lenguaje natural para creación de queries



Señales enriquecidas por IA

Nuestra IA analiza y enriquece las señales a través de múltiples atributos, identificando:

- Impersonated brands AI
- Companies mentioned and logos AI
- Content type and image descriptions AI
- Credentials requests AI
- Passwords and payment requests AI

Detección Typosquatting

Descubra amenazas ocultas

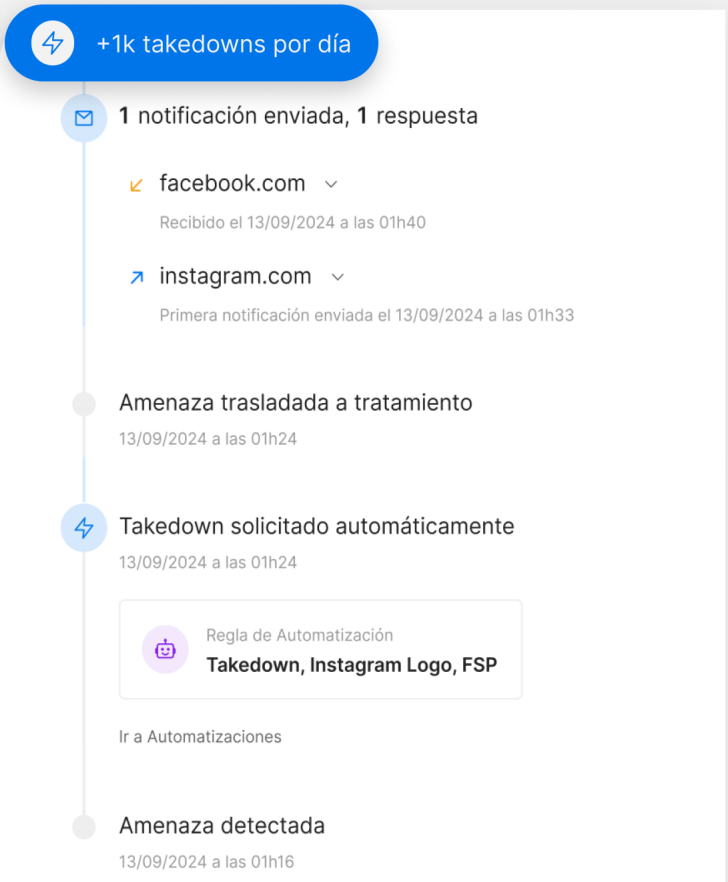
Supere las limitaciones basadas en palabras clave identificando variaciones de dominios engañosos diseñados para confundir a los usuarios. El Threat Hunting de Axur detecta el typosquatting y otras tácticas de manipulación de dominios, garantizando una detección integral de amenazas que los métodos tradicionales podrían pasar por alto. Esta detección avanzada lo mantiene protegido frente a tácticas sofisticadas utilizadas para evadir los sistemas de detección comunes.

Sin barreras de lenguaje

Detecte phishing en sitios en cualquier idioma, garantizando una protección global.

Detecte, evalue e retire los fraudes de phishing más rápido que nunca

- Takedown completamente automático
- Notificación en <4min
- 98,9% de éxito
- 9h de tiempo medio de resolución
- 15 dias de garantia de inactividad
- Web Safe Reporting
- Actualizaciones en todo el proceso
- Solamente cobramos el takedown exitoso



Listo para comprobarlo usted mismo?

SOLICITE UNA DEMOSTRACIÓN

bsi ISO/IEC 27001 Information Security Management CERTIFIED | CleanDNS Trusted Reporter

///AXUR

Descubra todas nuestras soluciones en **axur.com**