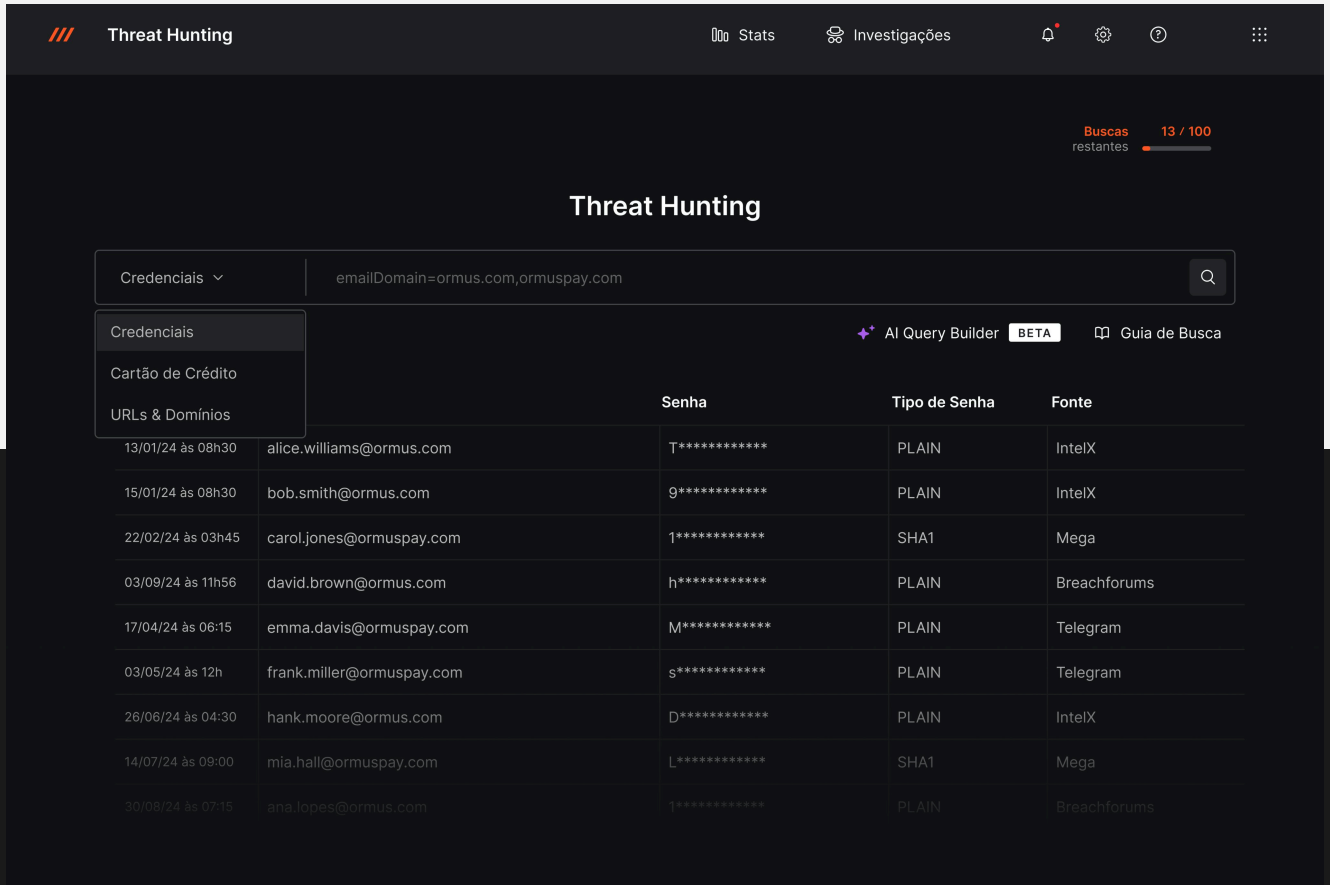
Threat Hunting

Melhore suas investigações com Threat Hunting em uma das maiores bases de ameaças do mundo

À medida que os ciberataques se tornam mais sofisticados, uma abordagem proativa é essencial. O Threat Hunting aprofunda-se em incidentes relevantes, ajudando a reduzir riscos e acelerar sua resposta a ataques.



Dados fictícios para fins de demonstração.

O Threat Hunting permite que você explore o amplo banco de dados da Axur, realizando buscas detalhadas por credenciais, cartões, arquivos vazados, URLs e domínios.

- Hunting proativo para investigar e interromper ameaças.
- Pesquisa de tendências para monitorar ataques no seu setor ou em concorrentes.
- Investigações de terceiros para avaliar a segurança de fornecedores e parceiros.

Descubra como o Threat Hunting pode fortalecer sua segurança

Credenciais

O Threat Hunting utiliza uma base de mais de 42 bilhões de credenciais expostas em vazamentos de dados e registros de malware, ajudando você a avaliar os riscos associados a fornecedores ou clientes, apoiar auditorias e prevenir acessos não autorizados por meio de senhas vazadas.

URLs & Domínios

O Threat Hunting revela sites de phishing e domínios maliciosos, mesmo sem menções explícitas de marcas. Isso permite detectar campanhas de phishing direcionadas, monitorar atividades de atores de ameaça e proteger proativamente contra novas ameaças online.

Cartões de crédito

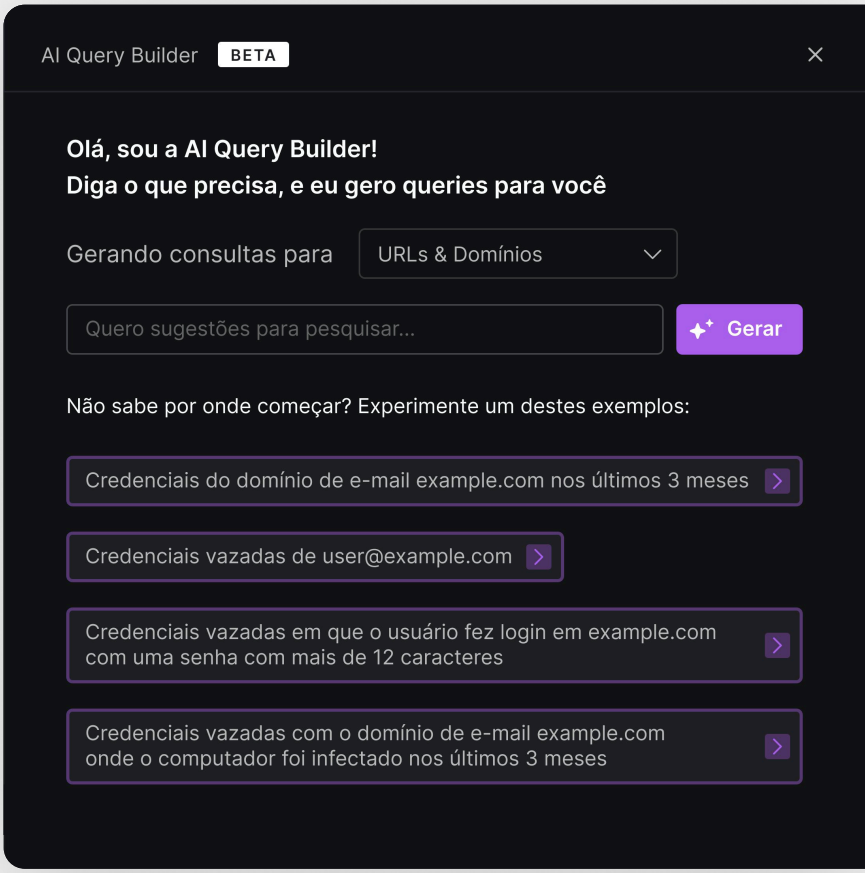
Busque informações de cartões de crédito vazados para identificar riscos de fraude precocemente. Essa abordagem auxilia empresas online a avaliar dados de pagamento expostos, sinalizar transações suspeitas e fortalecer medidas de proteção contra ameaças financeiras.

Apresentando o AI Query Builder:

Aproveite o poder da IA para criar consultas de forma rápida e eficiente.

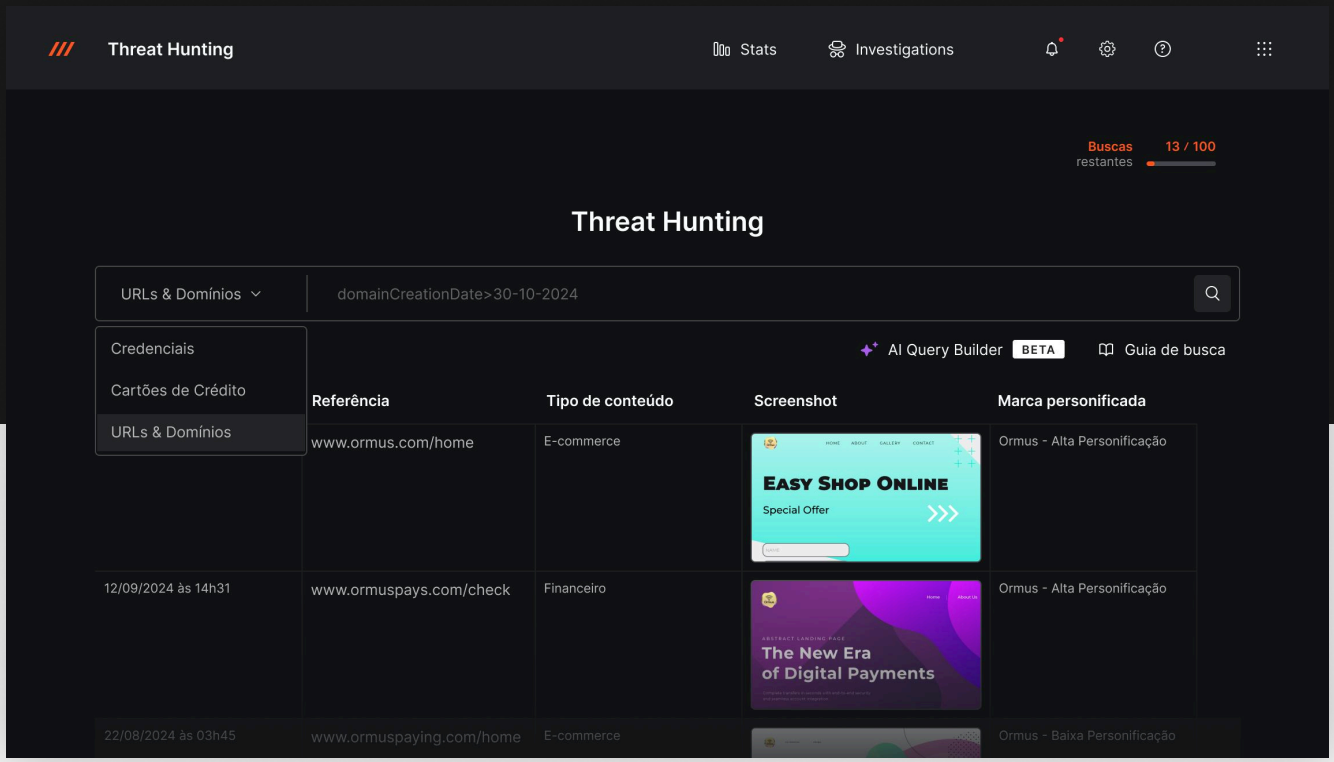
Suporta:

- ElasticSearch/ OpenSearch
- Conversão de linguagem natural em queries



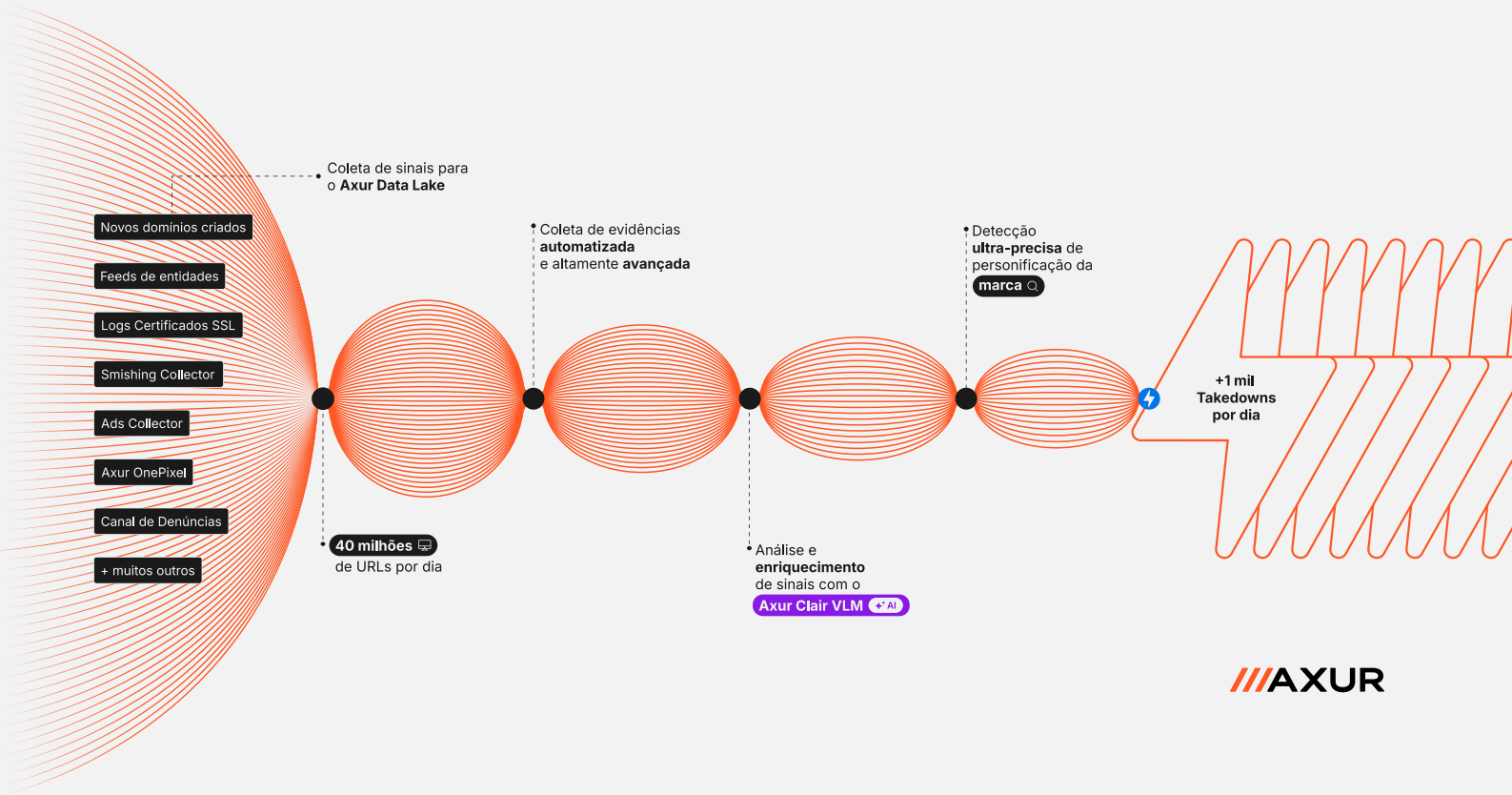
AXUR

O phishing está ficando mais complexo. E difícil de detectar



Uma abordagem totalmente nova em Brand Protection

Adicionamos 15 milhões de novos sites ao nosso data lake diariamente e usamos nossos modelos de GenAI para inspecionar e enriquecer cada sinal.



AXUR

Sinais enriquecidos por IA

Nossa IA analisa e enriquece sinais em diversos atributos, identificando:

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

Detecção de Typosquatting

Descubra ameaças ocultas

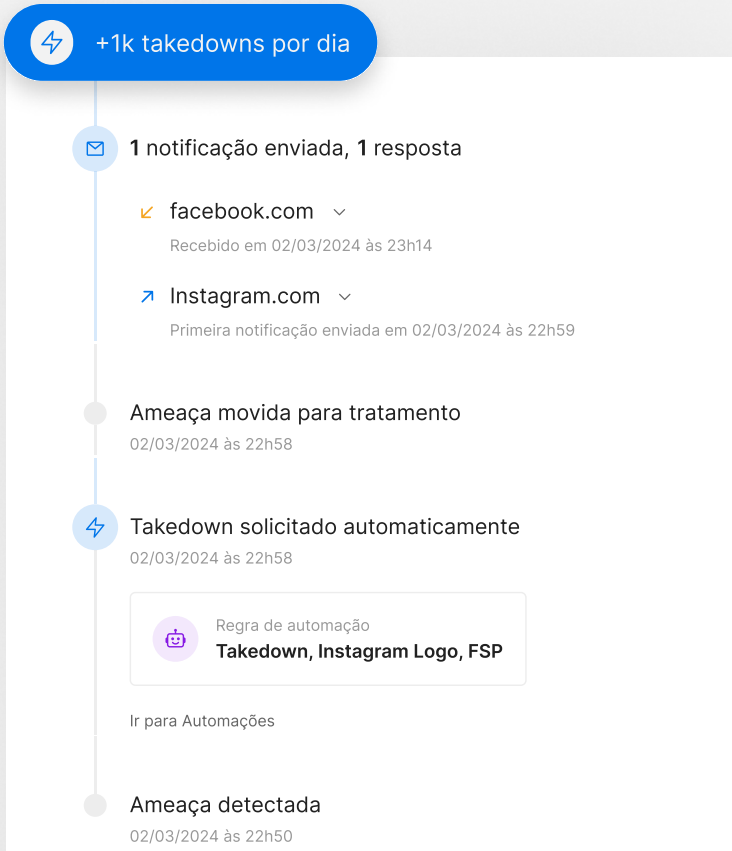
Supere as limitações de palavras-chave. Nossa solução identifica variações de domínio criadas para confundir usuários. O Threat Hunting detecta typosquatting e outras táticas de manipulação de domínio, garantindo uma detecção abrangente de ameaças que métodos tradicionais poderiam não perceber. Essa detecção avançada protege você contra táticas sofisticadas usadas para burlar sistemas tradicionais.

Sem barreiras de idiomas

Detecte sites de phishing em qualquer idioma, garantindo proteção global.

Detecte, avalie e derrube golpes de phishing mais rápido do que nunca

- Takedown completamente automatizado 24×7
- Notificação em <4 minutos
- 98,9% de sucesso
- 9h mediana de resolução
- 15 dias de garantia de permanência
- Web Safe Reporting
- Acompanhe todo o processo
- Pague apenas por takedowns bem-sucedidos



Pronto para ver na prática?

AGENDE UMA DEMO

Gartner Peer Insights 4.8

Descubra todas as nossas soluções em **axur.com**

AXUR