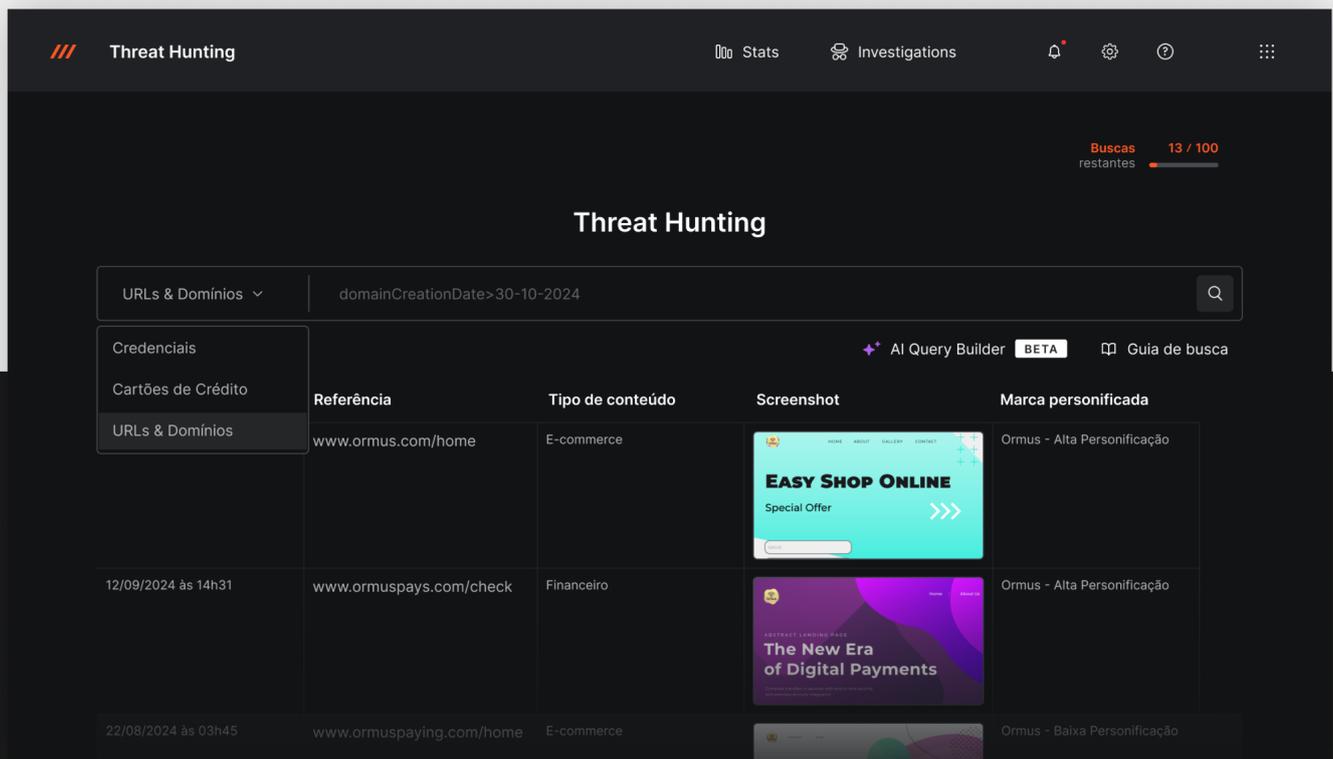


Faça hunting com o maior banco de dados de URLs maliciosas, enriquecido por Inteligência Artificial

Derrube cada ameaça com o melhor Takedown ⚡

Garanta que nenhuma ameaça passe despercebida com o maior banco de dados de URLs maliciosas, enriquecido por IA. Utilize o melhor takedown para remediar rapidamente cada uma delas, com proteção incomparável.



Dados fictícios para fins de demonstração.

Explore o extenso banco de dados da Axur, realizando buscas detalhadas por credenciais, cartões, arquivos vazados, URLs e domínios.

 Hunting proativo para interromper phishing de forma antecipada.

 Pesquisa de tendências para acompanhar ataques no seu setor ou concorrentes.

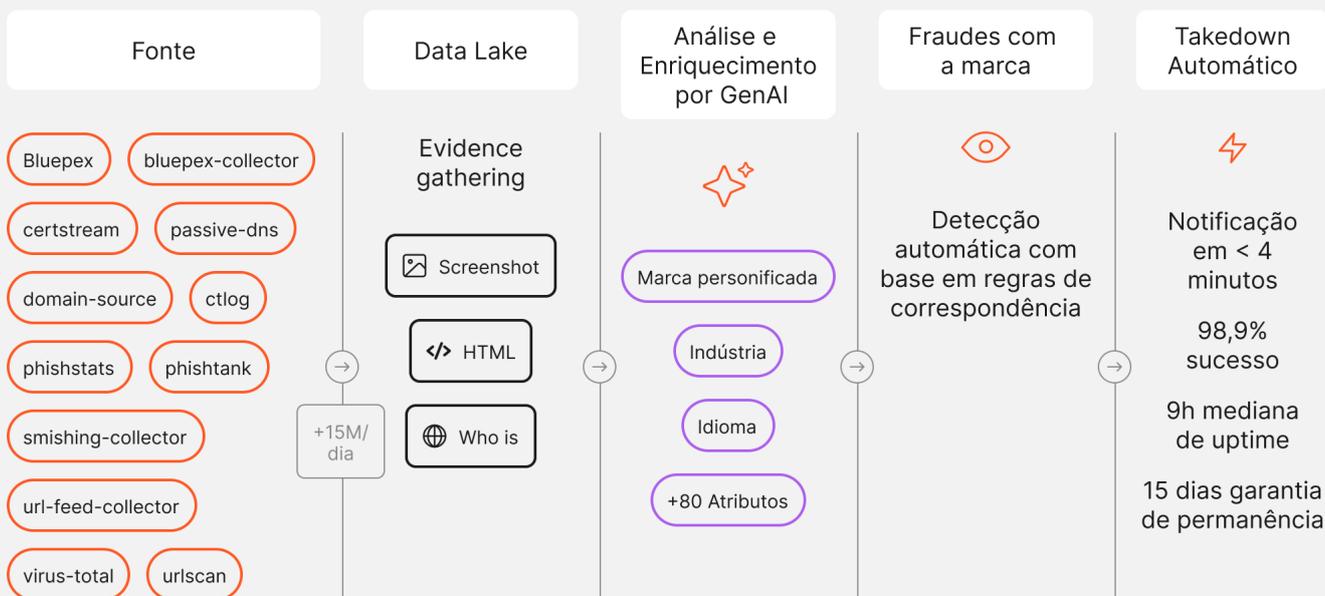
 Investigações de terceiros para avaliar a segurança de fornecedores e parceiros.

O phishing **está sofisticado.** E mais difícil de detectar

70% dos sites de phishing não usam nomes de marcas nos domínios, e 18% nem mesmo os mencionam no texto. A plataforma da Axur detecta cada uma dessas ameaças sofisticadas, indo além das palavras-chave para oferecer proteção completa.

Uma abordagem **totalmente nova** em Brand Protection

Adicionamos 15 milhões de novos sites à base diariamente. E usamos nossos modelos de GenAI para inspecionar e enriquecer cada sinal.



Aproveite a IA para criar queries sem esforço, tornando a investigação de ameaças rápida e fácil

ElasticSearch/
OpenSearch

Conversão de linguagem natural em queries

A interface da "AI Query Builder" (BETA) apresenta uma mensagem de boas-vindas e uma opção para gerar consultas para "URLs & Domínios". Um campo de busca sugere "Quero sugestões para pesquisar..." com um botão "Gerar". Abaixo, há exemplos de consultas pré-definidas:

- Credenciais do domínio de e-mail example.com nos últimos 3 meses
- Credenciais vazadas de user@example.com
- Credenciais vazadas em que o usuário fez login em example.com com uma senha com mais de 12 caracteres
- Credenciais vazadas com o domínio de e-mail example.com onde o computador foi infectado nos últimos 3 meses

O logo da AXUR é visível no canto inferior direito da interface.

Sinais enriquecidos por IA

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

Impersonated brands 

Companies mentioned and logos 

Content type and image descriptions 

Credentials requests 

Passwords and payment requests 

Detecção de Typosquatting

Descubra ameaças ocultas

Supere as limitações da busca por palavras-chave, identificando variações de domínios enganosos. O Threat Hunting da Axur detecta typosquatting e outras táticas de manipulação de domínios, garantindo a detecção completa de ameaças que métodos tradicionais podem não identificar. Essa detecção mantém você protegido contra táticas sofisticadas usadas para driblar a proteção tradicional.

Sem barreiras de linguagem

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

Detecte, avalie e remova phishings **mais rápido que nunca**

-  Takedown totalmente automatizado 24x7
-  Notificação em <4 minutos
-  98,9% de sucesso
-  9h mediana de uptime
-  Garantia de permanência de 15 dias
-  Web Safe Reporting
-  Acompanhe todo o processo
-  Pague apenas por takedowns bem-sucedidos

 +1k takedowns por dia

 1 notificação enviada, 1 resposta

 facebook.com 

Recebido em 13/09/2024 às 01h40

 instagram.com 

Primeira notificação enviada em 13/09/2024 às 01h33

Ameaça movida para tratamento

13/09/2024 às 01h24

 Takedown solicitado automaticamente

13/09/2024 às 01h24

 Automation rule
Takedown, Instagram Logo, FSP

Vá para Automações

Ameaça detectada

13/09/2024 às 01h16

Pronto para ver em prática?

FAÇA UMA DEMO



CleanDNS
Trusted Reporter 

///AXUR

Conheça todas as soluções em axur.com