

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.

The screenshot shows the Threat Hunting interface with a search bar containing the query 'emailDomain=ormus.com,ormuspay.com'. Below the search bar is a table of results:

		Senha	Tipo de Senha	Fonte
13/01/24 às 08h30	alice.williams@ormus.com	T*****	PLAIN	IntelX
15/01/24 às 08h30	bob.smith@ormus.com	g*****	PLAIN	IntelX
22/02/24 às 03h45	carol.jones@ormuspay.com	↑*****	SHA1	Mega
03/09/24 às 11h56	david.brown@ormus.com	h*****	PLAIN	Breachforums
17/04/24 às 06:15	emma.davis@ormuspay.com	M*****	PLAIN	Telegram
03/05/24 às 12h	frank.miller@ormuspay.com	s*****	PLAIN	Telegram
26/06/24 às 04:30	hank.moore@ormus.com	D*****	PLAIN	IntelX
14/07/24 às 09:00	mia.hall@ormuspay.com	L*****	SHA1	Mega
30/08/24 às 07:15	ana.lopes@ormus.com	↑*****	PLAIN	Breachforums

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.

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.

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.

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

AI Query Builder **BETA**

Olá, sou a AI Query Builder!
Diga o que precisa, e eu gero queries para você

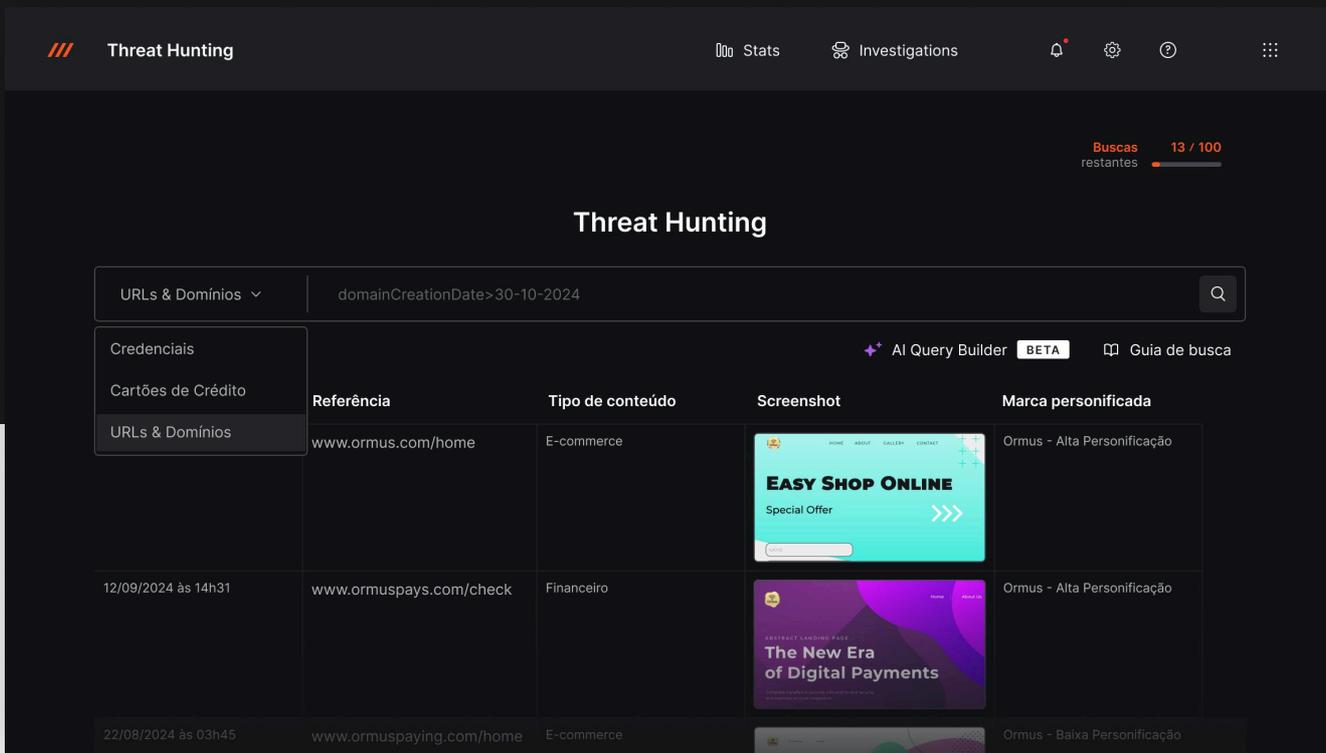
Gerando consultas para URLs & Domínios

Quero sugestões para pesquisar... **Gerar**

Não sabe por onde começar? Experimente um destes exemplos:

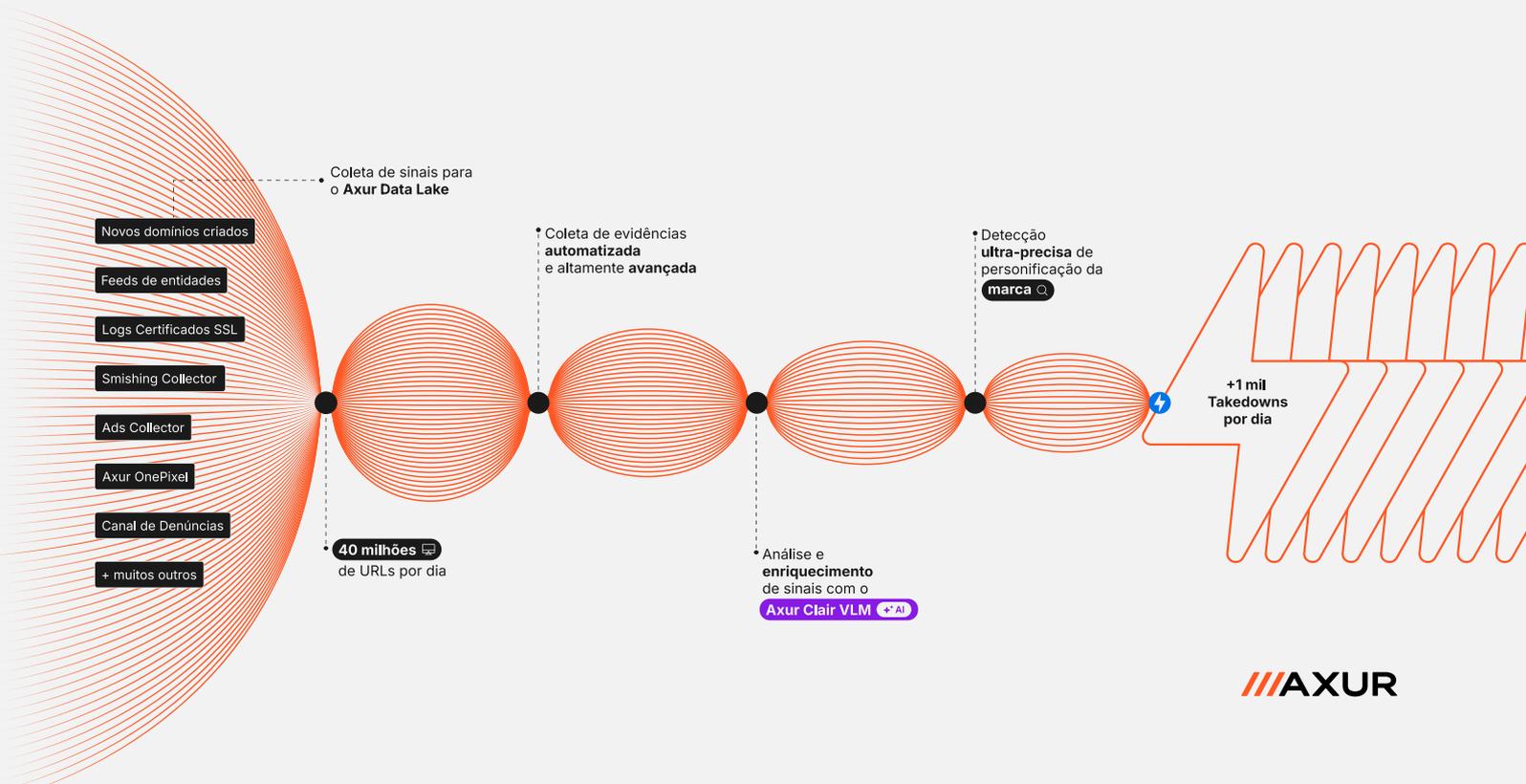
- Credenciais do domínio de e-mail example.com nos últimos 3 meses
- Credenciais vazadas de user@example.com
- Credenciais vazadas em que o usuário fez login em example.com com uma senha com mais de 12 caracteres
- Credenciais vazadas com o domínio de e-mail example.com onde o computador foi infectado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

O 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.



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 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 24x7
-  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

 +1k takedowns por dia

 1 notificação enviada, 1 resposta

 facebook.com ▾

Recebido em 02/03/2024 às 23h14

 Instagram.com ▾

Primeira notificação enviada em 02/03/2024 às 22h59

Ameaça movida para tratamento

02/03/2024 às 22h58

 Takedown solicitado automaticamente

02/03/2024 às 22h58



Regra de automação

Takedown, Instagram Logo, FSP

Ir para Automações

Ameaça detectada

02/03/2024 às 22h50

Pronto para ver na prática?

AGENDE UMA DEMO

Gartner
Peer Insights..  4.8
★★★★★



///AXUR

Descubra todas as nossas soluções em axur.com