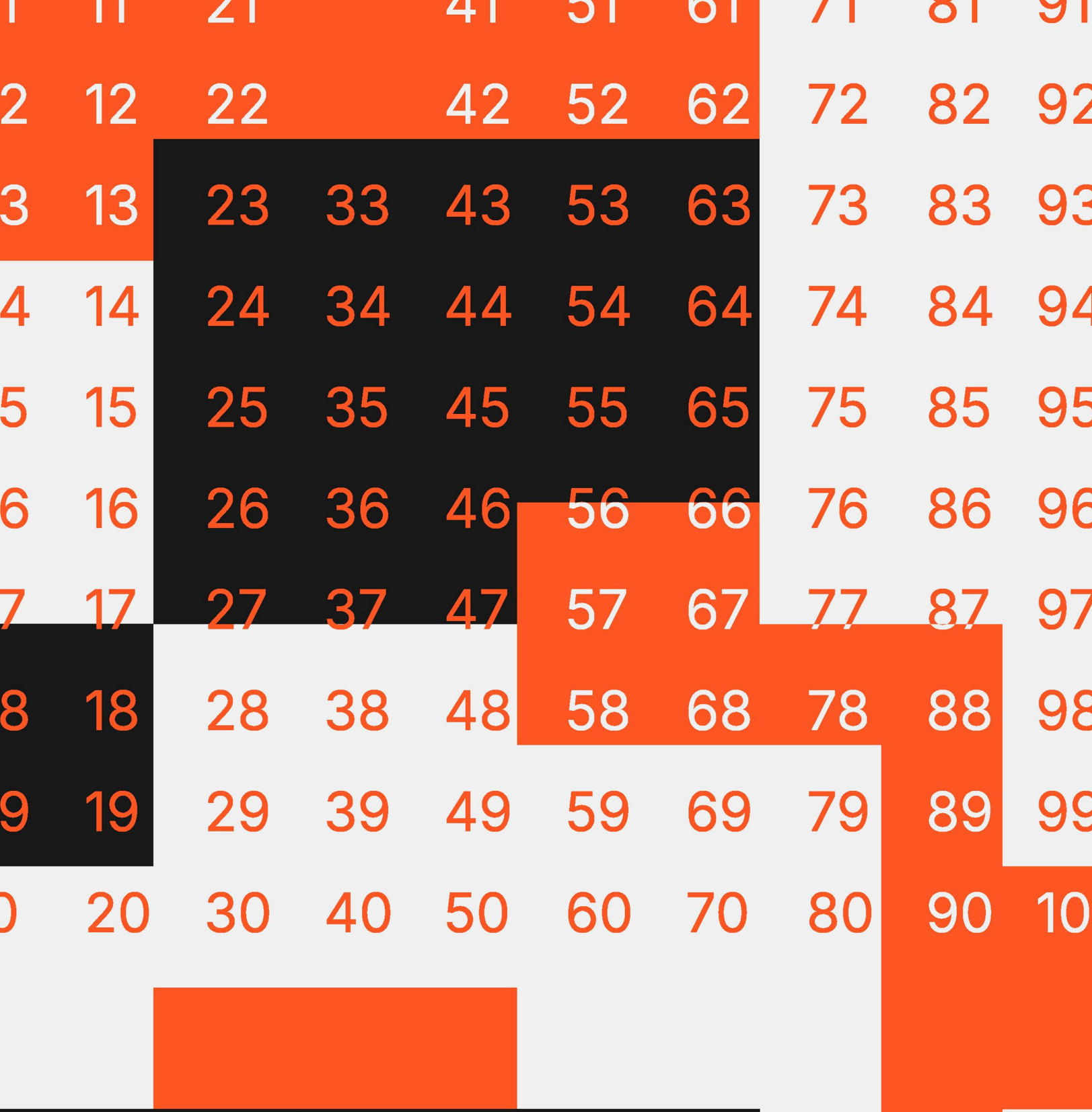



///AXUR

# 101 Casos de uso do Threat Hunting

# Sumário

# Casos de uso reais, resultado imediato

O Threat Hunting é uma ferramenta avançada de investigação da plataforma Axur. Ela permite que os usuários realizem buscas em uma riquíssima base de dados através de credenciais, cartões, anúncios, URLs e domínios. Para te ajudar a tirar mais valor da ferramenta, compilamos casos de uso reais de como nossos parceiros e clientes têm utilizado a solução para obter os melhores resultados.

## São 101 maneiras de fazer buscas e ter mais resultado nas suas investigações.

Busque por ameaças e incidentes dentro e fora dos seus ativos monitorados e aproveite todo o potencial da maior base de dados maliciosos, que conta com um modelo de IA que detecta visual e contextualmente ameaças em qualquer idioma para enriquecer e priorizar cada sinal.

- Casos de uso estratégicos
- Resposta à ameaças e incidentes
- Investigação profunda para mitigar riscos

Top Search **#01** Times: Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

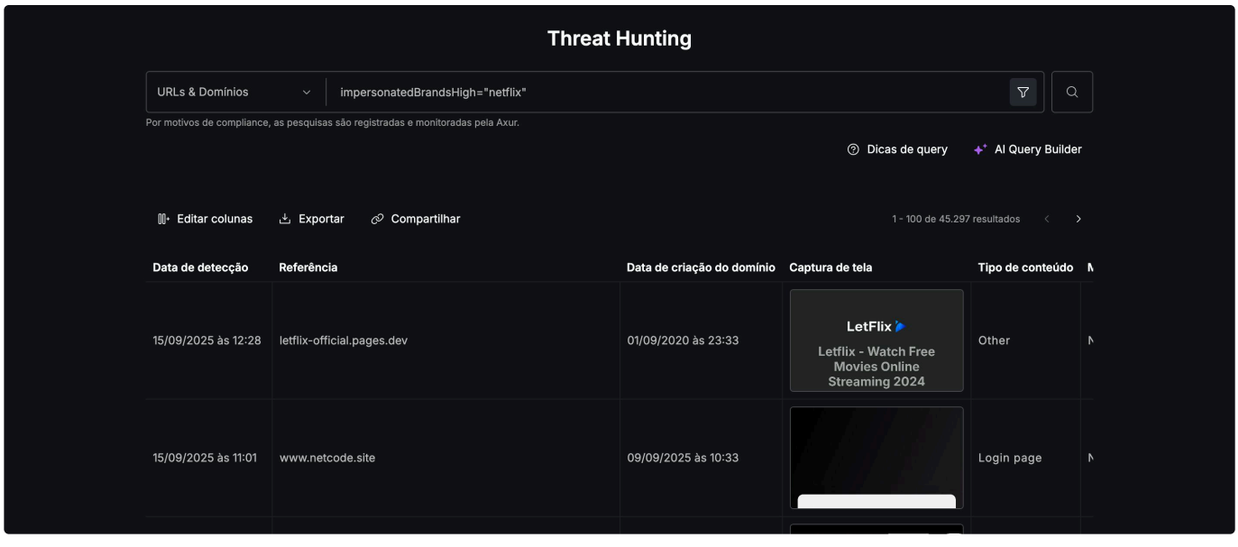
**Identificação de campanhas com alto nível de personificação visual e textual da identidade da empresa.**

Objetivo

Identificar campanhas com alto nível de personificação visual e textual, buscando domínios altamente associados à marca e páginas que simulam de forma evidente a identidade da empresa.

Busca

```
impersonatedBrandsHigh="{{company}}"
```




**#02** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Identificação de campanhas sazonais (e de concorrentes) por páginas relacionadas a datas comemorativas.**

Objetivo

Identificar campanhas sazonais amplas no setor, buscando páginas relacionadas a datas comemorativas. Como variação mais específica, é possível incluir competidores no filtro, por exemplo: `impersonatedBrandsHigh="amazon"`.

Busca

```
contentType=e-commerce AND detectionDate>=2025-04-01 AND "black friday"
```

**#03** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**URLs maliciosas recém-registradas no setor financeiro (adaptável a outros setores).**

Objetivo

Identificar URLs maliciosas registradas recentemente no setor financeiro, podendo ser adaptado para outros setores conforme a necessidade.

Busca

```
domainCreationDate>=2025-05-01 AND contentType=financial AND impersonatedBrandsHigh=*
AND passwordRequested="yes"
```

**#04** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso **Detecção de TLDs populares em golpes financeiros e e-commerce.**

Objetivo Identificar domínios com TLDs populares em golpes financeiros e de e-commerce, como .shop, buscando ameaças em sites que simulam lojas virtuais.

Busca `tld=shop AND impersonatedBrandsHigh={{company}}`

**#05** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso **Ameaças de phishing financeiro com domínios de pagamento.**

Objetivo Identificar ameaças de phishing financeiro que utilizam domínios com temática de pagamento, como TLD .pay, simulando páginas de pagamento.

Busca `tld=pay AND impersonatedBrandsHigh={{company}}`

**#06** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso **Domínios reservados para campanhas futuras e inativos.**

Objetivo Identificar domínios reservados como preparação para campanhas futuras, buscando aqueles registrados nos últimos 90 dias que estão inativos, sem conteúdo ou marcados como "parked".

Busca `contentType="error page" AND companiesMentioned={{company}}`

**#07** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso **Domínios que retornam erro para ataques de desligamento.**

Objetivo Identificar domínios que retornam erro e podem ser usados em ataques que “ligam e desligam” páginas falsas em determinados horários, buscando por páginas classificadas como “error page”.

Busca `contentType="error page" AND companiesMentioned={{company}}`

**#08** Times: Legal, Compliance Contexto: URLs & Domínios

Caso de uso

**Domínios relacionados a atividades de apostas com marca da empresa.**

Objetivo

Identificar domínios relacionados a atividades de apostas que utilizam ou associam a marca da empresa, buscando conteúdo classificado como “gambling” e que contenha menções à marca nesse contexto.

Busca

```
contentType="gambling" AND companiesMentioned={{company}}
```

**#09** Times: Legal, Compliance Contexto: URLs & Domínios

Caso de uso

**Domínios que aparentam ser fontes de notícia para desinformação.**

Objetivo

Investigar domínios que aparentam ser fontes de notícia, buscando conteúdo do tipo “news” onde a empresa é mencionada na imagem ou no HTML. Esses sites podem imitar grandes portais de notícia para desinformação ou manipulação. Como variação, é possível buscar apenas pelo uso do logo da empresa, por exemplo: `companyLogo={{company}}`.

Busca

```
contentType="news" AND companiesMentioned={{company}}
```

**#10** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Páginas financeiras falsas que imitam bancos e fintechs.**

Objetivo

Detectar páginas financeiras falsas que simulam instituições legítimas, podendo ser aplicado a uma empresa específica ou a todo o setor financeiro. A busca pode ser feita por conteúdo classificado como “financial”, identificando páginas que imitam bancos, fintechs ou operadoras de cartão.

Busca

```
contentType="financial" AND impersonatedBrand={{company}}
```

**#11** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Páginas falsas de login para capturar credenciais.**

Objetivo

Identificar páginas falsas de login criadas para capturar credenciais, buscando conteúdo classificado como “login page”.

Busca

```
contentType="login page" AND impersonatedBrand={{company}}
```

#12 Times: Legal, Compliance Contexto: URLs & Domínios

Caso de uso

**Golpes de e-commerce falso com produtos inexistentes.**

Objetivo

Identificar golpes que utilizam páginas de e-commerce falsas com produtos inexistentes ou clonados, buscando conteúdo classificado como “e-commerce” em páginas que mencionam a empresa e estão em domínios registrados nos últimos 90 dias.

Busca

```
contentType="e-commerce" AND companiesMentioned={{company}} AND
domainCreationDate>2025-06-30
```

#13 Times: Legal, Compliance Contexto: URLs & Domínios

Caso de uso

**Páginas com conteúdo adulto associadas à marca da empresa.**

Objetivo

Identificar páginas com conteúdo adulto que associam a marca da empresa, buscando por páginas classificadas como “adult” que mencionam a empresa.

Busca

```
contentType="adult" AND companiesMentioned={{company}}
```

#14 Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Domínios e hosts que utilizam a marca no nome exato.**

Objetivo

Identificar domínios e hosts que utilizam a marca, buscando pela presença exata do nome da marca no domínio ou host.

Busca

```
(domainLabel={{company}} OR subdomain={{company}})
```

#15 Times: Blue Team Contexto: URLs & Domínios

Caso de uso

**Campanhas de phishing operadas a partir de uma mesma região geográfica.**

Objetivo

Mapear campanhas de phishing operadas a partir de uma mesma região geográfica, utilizando dados de geolocalização para identificar clusters de ataques associados à marca, hospedados em ISPs específicos, como na Rússia.

Busca

```
impersonatedBrandsHigh={{company}} AND geolocationCountryName="Russia"
```

Top Search #16 — Times: Blue Team, Anti-Fraud Team — Contexto: URLs & Domínios

Caso de uso

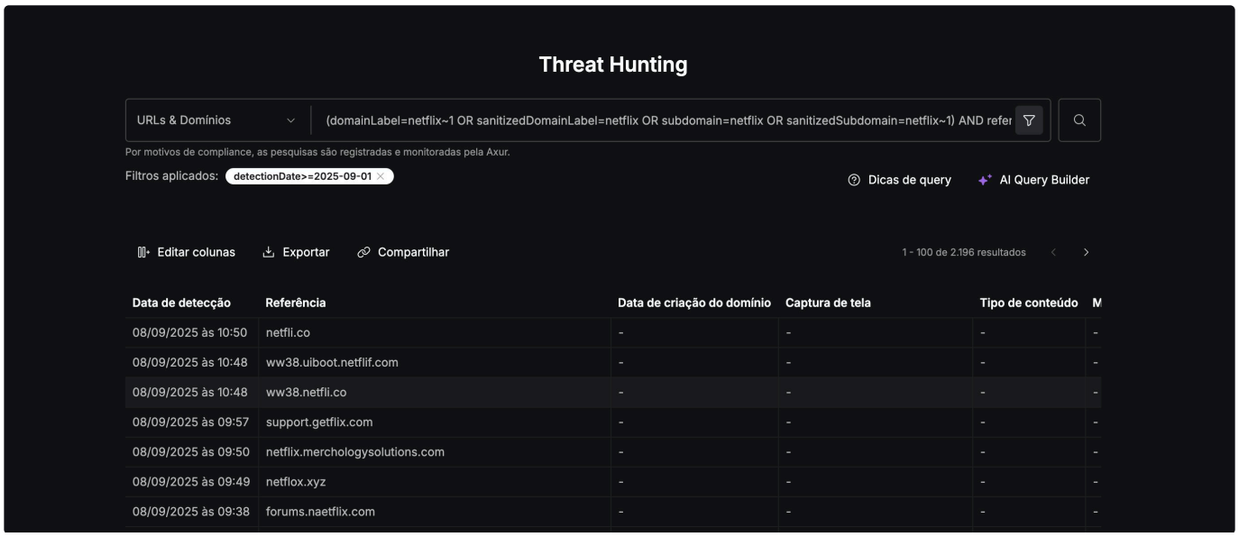
**Domínios e hosts similares à marca com variações e homóglifos.**

Objetivo

Identificar domínios e hosts similares à marca, buscando pela presença da marca no domínio com variações, incluindo typos e homoglifos.

Busca

```
(domainLabel={{company}}~1 OR sanitizedDomainLabel={{company}} OR subdomain={{company}}~1
OR sanitizedSubdomain={{company}}~1) AND referenceType=DOMAIN
```




#17 — Times: Blue Team — Contexto: URLs & Domínios

Caso de uso

**Campanhas de phishing operadas a partir de uma mesma região geográfica.**

Objetivo

Mapear campanhas de phishing originadas de uma mesma região geográfica, utilizando dados de geolocalização para identificar clusters de ataques associados a páginas de login da Microsoft e da Apple, hospedados em ISPs na Rússia.

Busca

```
(impersonatedBrandsHigh=Microsoft OR impersonatedBrandsHigh=Apple)
AND contentType="login page" AND  geolocationCountryName="Russia"
```

#18 — Times: Blue Team — Contexto: URLs & Domínios

Caso de uso

**Campanhas de phishing que utilizam o mesmo ISP.**

Objetivo

Investigar campanhas de phishing que utilizam o mesmo ISP, identificando páginas falsas que compartilham a mesma infraestrutura de hospedagem.

Busca

```
impersonatedBrandsHigh={{company}} AND isp="Cloudflare"
```

Top Search **#19** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

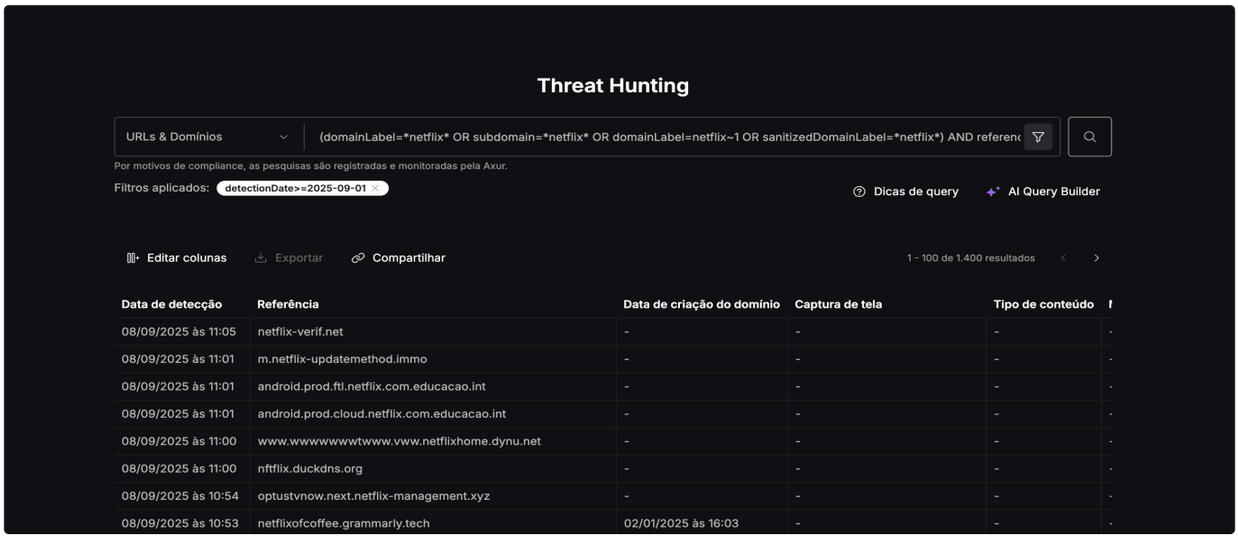
**Busca ampla de domínios similares com grande volume de detecções.**

Objetivo

Identificar domínios e hosts similares à marca, buscando pela presença da marca em qualquer parte do domínio com variações, incluindo typos e homoglifos. Dependendo da marca, essa busca pode gerar um volume muito grande de detecções.

Busca

```
(domainLabel=*netflix* OR subdomain=*netflix* OR domainLabel=netflix~1
OR sanitizedDomainLabel=*netflix*) AND referenceType=DOMAIN
```




**#20** Times: Blue Team Contexto: URLs & Domínios

Caso de uso

**Páginas que solicitam dados de pagamento associadas à marca.**

Objetivo

Analisar páginas que solicitam dados de pagamento associadas à marca, buscando por páginas com formulários de pagamento vinculados à empresa ou ao setor.

Busca

```
impersonatedBrandsHigh="{{company}}" AND paymentRequested="yes"
AND domainCreationDate<=2025-06-10
```

**#21** Times: Blue Team Contexto: URLs & Domínios

Caso de uso

**URLs que utilizam marcas Visa, Mastercard e a marca da empresa.**

Objetivo

Investigar URLs que utilizam as marcas Visa, Mastercard e a marca da empresa, buscando páginas em que Visa ou Mastercard são mencionadas em conjunto com a marca da empresa.

Busca

```
companyLogo=("Visa" OR "Mastercard") AND impersonatedBrandsHigh="Bank of America"
```

#22 Times: Blue Team Contexto: URLs & Domínios

Caso de uso

**Validação de URL suspeita em múltiplas bases especializadas.**

Objetivo

Validar se uma URL suspeita consta em múltiplas bases especializadas de phishing, verificando se o domínio já é listado como malicioso e obtendo uma confirmação com maior cobertura.

Busca

```
origin=("phishtank" OR "phishstats" OR "apwg-collector" OR "smishing-collector")
AND domain={{domain.com}}
```

#23 Times: Blue Team, Anti-Fraud Team Contexto: Ads & Paid Search

Caso de uso

**Páginas maliciosas promovidas por campanhas pagas no Facebook Ads.**

Objetivo

Investigar páginas maliciosas promovidas por campanhas pagas no Facebook Ads, identificando URLs falsas patrocinadas que utilizam a marca e consolidando uma lista dessas URLs anunciadas.

Busca

```
origin=("facebook-ads-coll" OR "paid search" OR "browser-bar")
AND impersonatedBrandsHigh={{company}}
```

#24 Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Campanhas ligadas ao mesmo perfil após detecção de fraude.**

Objetivo

Buscar campanhas ligadas ao mesmo perfil após a detecção de fraude via anúncios do Facebook Ads, mapeando o histórico de campanhas fraudulentas associadas ao mesmo operador.

Busca

```
metaProfileName="{{Fraudster Name}}"
```

#25 Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Fraudes promovidas pelo mesmo link de anunciante após campanha enganosa.**

Objetivo

Buscar fraudes promovidas pelo mesmo link de anunciante após uma campanha enganosa, rastreando outras campanhas associadas à mesma URL e consolidando uma lista de campanhas fraudulentas veiculadas pelo mesmo perfil.

Busca

```
metaAdvertiserProfiles="https://facebook.com/discount-amazon-store"
```

Top Search **#26** Times: Blue Team, Anti-Fraud Team, Legal, Compliance Contexto: URLs & Domínios

Caso de uso

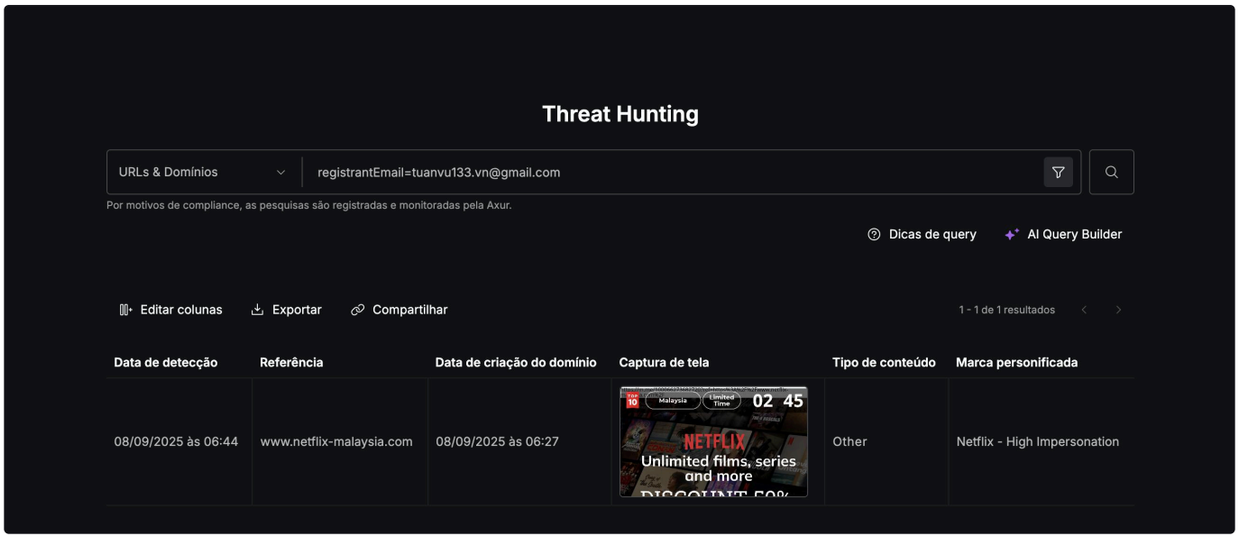
**Páginas maliciosas associadas ao mesmo registrante ou e-mail.**

Objetivo

Investigar páginas maliciosas associadas ao mesmo registrante ou e-mail de registro, buscando fraudes de campanhas que reutilizam informações de cadastro WHOIS e identificando potenciais páginas fraudulentas criadas pelo mesmo registrante.

Busca

```
registrantEmail="{{fraudstermail.com}}"
```




**#27** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Campanhas recentes hospedadas por provedores como Cloudflare.**

Objetivo

Investigar campanhas recentes hospedadas por provedores como Cloudflare, correlacionando ameaças que utilizam a mesma infraestrutura de hospedagem e identificando domínios maliciosos recentes associados ao mesmo ISP.

Busca

```
isp=Cloudflare AND impersonatedBrandsHigh="{{company}}" AND
domainCreationDate>=2025-06-01
```

**#28** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Campanhas que compartilham a mesma infraestrutura de DNS.**

Objetivo

Investigar campanhas que compartilham a mesma infraestrutura de DNS, buscando domínios associados a campanhas anteriores que utilizam o mesmo name server e identificando possíveis fraudes relacionadas pela reutilização de DNS.

Busca

```
nameServers="ns1.fraudns.org" AND nameServers="ns2.fraudns.org"
```

#29 Times: Blue Team Contexto: URLs & Domínios

Caso de uso

**Páginas potencialmente utilizadas para capturar credenciais corporativas.**

Objetivo

Identificar páginas potencialmente utilizadas para capturar credenciais corporativas, buscando páginas falsas de plataformas como Google e Microsoft em domínios que mencionam a marca do cliente.
O objetivo é detectar campanhas de phishing direcionadas a funcionários para roubo de credenciais de acesso corporativo.

Busca

```
impersonatedBrandsHigh=(microsoft OR google) AND credentialRequested="yes"
AND domain=*{{company}}*
```

#30 Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Domínios possivelmente usados para spear phishing sem página web ativa.**

Objetivo

Identificar domínios possivelmente usados para spear phishing, buscando domínios que personificam a marca da empresa, possuem registros MX configurados para envio de e-mails, mas não têm página web ativa.

Busca

```
dnsRecordType="MX" AND domain=*{{company}}*
```

#31 Times: Legal, Compliance Contexto: URLs & Domínios

Caso de uso

**Vinculação da marca a conteúdos impróprios como jogos de azar.**

Objetivo

Identificar a vinculação da marca a conteúdos impróprios, como jogos de azar, buscando por páginas classificadas como “gambling” que exibem o logo da marca.

Busca

```
contentType=gambling AND companyLogo={{company}}
```

#32 Times: Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Páginas potencialmente utilizadas para fraudes em outros países.**

Objetivo

Identificar páginas potencialmente utilizadas para fraudes em outros países, buscando páginas que personificam a marca em idiomas diferentes e em regiões onde a empresa não atua.

Busca

```
companyLogo="{{company}}" AND NOT predominantLanguage=english
```

#33 Times: Blue Team Contexto: URLs & Domínios

Caso de uso

**Conteúdo malicioso hospedado em subdomínios próprios inativos.**

Objetivo

Descobrir conteúdo malicioso hospedado em subdomínios próprios que deveriam estar inativos, buscando casos de subdomain hijacking. A investigação deve gerar uma lista de subdomínios da empresa configurados com registros CNAME apontando para provedores de hospedagem de terceiros, permitindo avaliar quais estão vulneráveis ou sendo usados de forma indevida.

Busca

```
domain={{company.com}} AND (dnsRecordType=CNAME AND dnsRecordValue=(*.github.io OR
*.herokuapp.com OR *.s3.amazonaws.com OR *.cloudfront.net OR *.wordpress.com))
```

#34 Times: Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Detecção de domínios com uso exclusivo de IPv6 e registro AAAA para identificar configurações intencionais de evasão**

Objetivo

Identificar domínios que utilizam exclusivamente IPv6 e mencionam a empresa, buscando domínios suspeitos com apenas registro AAAA. O uso exclusivo de IPv6 pode indicar uma configuração intencional para evitar detecção, já que algumas ferramentas e firewalls ainda oferecem menor cobertura para IPv6.

Busca

```
dnsRecordType="AAAA" AND NOT dnsRecordType=A AND companiesMentioned=google
```

#35 Times: Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Páginas com uso indevido do logo da marca sem menção textual no domínio.**

Objetivo

Identificar páginas que utilizam o logo da marca sem mencionar o nome da marca na URL, buscando uso indevido de elementos visuais sem relação textual no domínio.

Busca

```
companyLogo={{company}} AND NOT reference=*{{company}}*
```

#36 Times: Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Domínios recentes (60 dias) que utilizam a marca em suas páginas.**

Objetivo

Identificar páginas que utilizam a marca, buscando domínios registrados nos últimos 60 dias que contenham páginas fazendo uso da marca.

Busca

```
domainCreationDate>=2025-07-01 AND companiesMentioned={{company}}
```

Top Search **#37** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

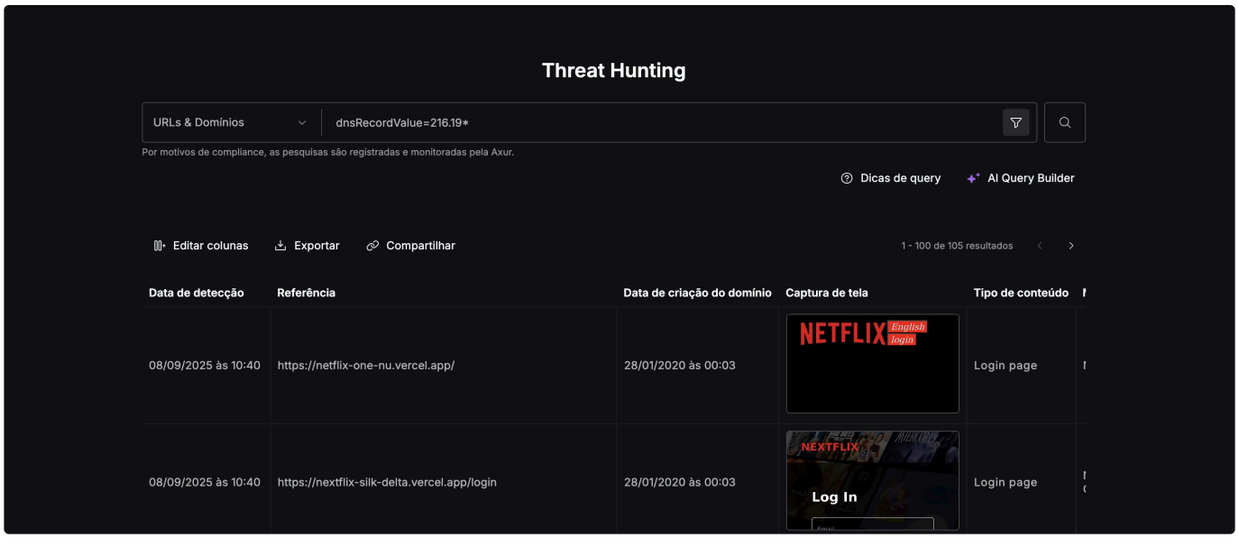
**Campanhas que compartilham mesmo bloco de IPs.**

Objetivo

Investigar campanhas que compartilham o mesmo bloco de IPs (sextetos ou octetos), buscando, a partir de uma página falsa identificada, outras páginas associadas à mesma infraestrutura.

Busca

```
dnsRecordValue=18.230*
```




**#38** Times: Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Uso indevido de nomes de executivos para promoção não autorizada de produtos ou serviços.**

Objetivo

Verificar o uso indevido de nomes de executivos fora de contextos jornalísticos, buscando páginas que exploram esses nomes para promover a venda de produtos ou serviços sem autorização.

Busca

```
"Bill Gates" AND "bitcoin"
```

**#39** Times: Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Investigação de sites falsos que imitam suporte técnico da empresa para capturar dados pessoais.**

Objetivo

Investigar casos em que clientes afirmam ter inserido dados pessoais em sites falsos que imitavam o suporte técnico da empresa, buscando páginas que mencionam a marca, solicitam senha e simulam atendimento ao usuário, contendo palavras como “help” ou “customer” na URL.

Busca

```
impersonatedBrandsHigh="{{company}}" AND reference=(*help* OR *customer*)
```

**#40** Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

**Caso de uso**

**Páginas falsas de concorrentes (especialmente logins) para antecipar ataques.**

**Objetivo**

Identificar ataques de páginas falsas contra competidores para antecipar ameaças, buscando por páginas com alto nível de personificação dessas marcas, registradas nos últimos 90 dias. Como variação mais específica, é possível filtrar apenas páginas cujo `contentType="login page"`, priorizando aquelas que imitam áreas de autenticação dos competidores.

**Busca**

```
(impersonatedBrandsHigh="competidor A" OR impersonatedBrandsHigh="competidor B")
AND domainCreationDate>2025-06-30
```

**#41** Times: Anti-Fraud Team Contexto: URLs & Domínios

**Caso de uso**

**Identificação de campanhas com uso parcial de elementos da marca e média personificação.**

**Objetivo**

Identificar campanhas com uso parcial de elementos da marca, buscando fraudes com média personificação, em páginas que apresentam elementos moderadamente relacionados à marca. Essa abordagem pode gerar um volume maior de casos, mas é útil para identificar situações fora do padrão.

**Busca**

```
impersonatedBrandsMedium="{{company}}"
```

**#42** Times: Anti-Fraud Team Contexto: URLs & Domínios

**Caso de uso**

**Detecção de campanhas iniciais ou sutis com personificação de baixo nível da marca.**

**Objetivo**

Detectar campanhas iniciais ou sutis que utilizam a marca, buscando casos de personificação de baixo nível. Essa abordagem pode gerar um volume maior de resultados, mas é útil para identificar ameaças em estágio inicial ou situações fora do padrão.

**Busca**

```
impersonatedBrandsLow="{{company}}"
```

**#43** Times: Anti-Fraud Team Contexto: URLs & Domínios

**Caso de uso**

**Identificação de páginas que mencionam a empresa em sites classificados como "finance".**

**Objetivo**

Identificar páginas que mencionam a empresa em seu conteúdo textual ou visual, buscando menções à marca em sites classificados como “financial”.

**Busca**

```
companiesMentioned="{{company}}" AND contentType="financial"
```

#44 Times: Anti-Fraud Team Contexto: URLs & Domínios

| | |
|---|---|
| Caso de uso | **Verificação do uso do logotipo da empresa em domínios potencialmente maliciosos classificados como "financial".** |
| Objetivo | Verificar o uso do logotipo da empresa em domínios potencialmente maliciosos, buscando a presença de elementos visuais da marca em sites classificados como “finance”. |
| Busca | `companyLogo="{{company}}" AND contentType="financial"` |

#45 Times: Anti-Fraud Team Contexto: URLs & Domínios

| | |
|---|---|
| Caso de uso | **Rastreamento de simulações visuais de aplicativos que mencionam o nome da marca da empresa.** |
| Objetivo | Rastrear simulações visuais de aplicativos, buscando páginas com aparência de apps que mencionam o nome da marca da empresa. |
| Busca | `imageDescription=({{company}} AND "mobile app")` |

#46 Times: Anti-Fraud Team Contexto: URLs & Domínios

| | |
|---|---|
| Caso de uso | **Detecção de domínios com links para o Telegram que mencionam a marca da empresa.** |
| Objetivo | Detectar domínios que possuem links para o Telegram e mencionam a marca, buscando páginas que fazem referência à empresa e contêm links HTML externos apontando para grupos ou perfis no Telegram. |
| Busca | `htmlLinks=t.me AND companiesMentioned="{{company}}"` |

#47 Times: Anti-Fraud Team Contexto: URLs & Domínios

| | |
|---|---|
| Caso de uso | **Identificação de páginas que redirecionam para números ou grupos do WhatsApp para golpes diretos.** |
| Objetivo | Identificar páginas que redirecionam para números ou grupos do WhatsApp, detectando golpes realizados por meio de contatos diretos na plataforma. A busca gera uma lista de páginas que incentivam a comunicação direta com golpistas via WhatsApp. |
| Busca | `impersonatedBrandsHigh="{{company}}" AND htmlLinks=wa.me` |

#48 Times: Anti-Fraud Team Contexto: URLs & Domínios

**Caso de uso**

**Investigação de fraudes organizadas em servidores ou grupos do Discord com links HTML.**

**Objetivo**

Investigar fraudes organizadas em servidores ou grupos do Discord, identificando páginas que contêm links HTML referenciando grupos na plataforma. O objetivo é detectar campanhas ou comunidades ilegítimas operando por meio do Discord.

**Busca**

```
impersonatedBrandsHigh="{{company}}" AND htmlLinks=discord.gg
```

#49 Times: Anti-Fraud Team Contexto: URLs & Domínios

**Caso de uso**

**Identificação de fraudes que direcionam vítimas para números do WhatsApp e rastreamento de campanhas associadas.**

**Objetivo**

Identificar fraudes que direcionam vítimas para números no WhatsApp, e, a partir da detecção de um número fraudulento, rastrear outras páginas associadas à mesma campanha criminosa.

**Busca**

```
htmlLinks=*11922331092*
```

#50 Times: Anti-Fraud Team Contexto: URLs & Domínios

**Caso de uso**

**Domínios ativos maliciosos que personificam a marca, especialmente recentes e operacionais.**

**Objetivo**

Identificar domínios ativos e maliciosos que personificam a marca, especialmente aqueles criados recentemente e que ainda estão operacionais (não suspensos).

**Busca**

```
impersonatedBrandsHigh="{{company}}" AND domainCreationDate>=2025-06-01
AND NOT domainStatus="suspended"
```

#51 Times: Anti-Fraud Team Contexto: URLs & Domínios

**Caso de uso**

**Páginas com encurtadores de URL que mascaram ataques mencionando a marca.**

**Objetivo**

Identificar e detectar páginas que usam encurtadores (como Bit.ly, TinyURL, etc.) para mascarar URLs finais, mencionando uma marca e utilizando esses redirecionadores populares como ponte para ataques, listando os URLs envolvidos.

**Busca**

```
htmlLinks=("bit.ly" OR "tinyurl.com" OR "t.co" OR "cutt.ly" OR "is.gd")
AND companiesMentioned="{{company}}"
```

#52 Times: Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso **Tentativas de phishing com domínios similares à empresa usando operador "fuzzy".**

Objetivo Identificar possíveis tentativas de phishing buscando por domínios similares à sua empresa (com o operador "fuzzy"), para listar domínios semelhantes a "company" que possam estar sendo usados para enganar usuários.

Busca `reference={{company}}~1 AND NOT domain={{company.com}}`

#53 Times: Blue Team Contexto: Credenciais

Caso de uso **Táticas de coleta de credenciais do setor e credenciais vazadas de websites específicos.**

Objetivo Mapear táticas de coleta de credenciais comuns no setor e identificar credenciais vazadas de acesso a um website específico, usando apenas o domínio ou a URL completa.

Busca `accessUrl={{company.com}}`

#54 Times: Red & Blue Teams, Legal Contexto: Credenciais

Caso de uso **Risco de segurança de fornecedores através de exposição de credenciais de colaboradores.**

Objetivo Avaliar o risco de segurança ao contratar um fornecedor, buscando por exposição de credenciais de seus colaboradores.

Busca `emailDomain={{company.com}}`

#55 Times: Red & Blue Teams Contexto: Credenciais

Caso de uso **Exposição prévia de colaborador em fontes de alto risco e deep/dark web.**

Objetivo Identificar a exposição prévia de um colaborador em fontes de alto risco, buscando vazamentos relacionados a um usuário específico, determinando a fonte, que pode ser a deep/dark web.

Busca `user="{{user@company.com}}" AND sourceName="Deep/Dark Web"`

#56 Times: Blue Team Contexto: Credenciais

Caso de uso **Credenciais vazadas com URL de acesso testável.**

Objetivo Verificar se uma credencial vazada tem URL de acesso disponível, buscando por credenciais expostas da sua empresa que estejam associadas a uma URL de acesso e que possam ser testadas imediatamente nessa URL.

Busca `user="{{user@company.com}}" AND accessUrl=*`

#57 Times: Blue Team Contexto: Credenciais

Caso de uso **Credenciais vazadas em um arquivo específico.**

Objetivo Explorar arquivos com grandes volumes de credenciais à venda em fóruns, e a partir dessa busca, avaliar que outras credenciais são provenientes de um arquivo específico para entender seu conteúdo, o perfil das vítimas e as possíveis conexões.

Busca `fileName="830k DUMP MIX.txt"`

#58 Times: Blue Team, Legal Contexto: Credenciais

Caso de uso **Análise de riscos de parceiros estratégicos em vazamentos externos.**

Objetivo Investigar a exposição de parceiros estratégicos em vazamentos externos, avaliando o impacto indireto de vazamentos estruturados sobre esses parceiros para mapear o risco por associação com terceiros.

Busca `fileName="leaked_suppliers.txt" AND *{{vendor}}*`

#59 Times: Blue Team Contexto: Credenciais

Caso de uso **Exposição de credenciais corporativas por e-mail profissional.**

Objetivo Verificar se uma credencial corporativa foi exposta por e-mail profissional, buscando por todas as credenciais expostas usando o e-mail completo de um indivíduo.

Busca `user="john.doe@company.com"`

**#60** Times: Anti-Fraud Team, Blue Team — Contexto: Credenciais

| | |
|---|---|
| Caso de uso | **Presença de números de telefone em vazamentos com credenciais associadas.** |
| Objetivo | Verificar a presença do número de telefone de um cliente em vazamentos, buscando por telefones com identificação de username e verificando se existem credenciais associadas, o que é muito interessante em processos de investigação e fraude. |
| Busca | `user="{{+5511987654321}}" AND userType="PHONE"` |

**#61** Times: Blue Team — Contexto: Credenciais

| | |
|---|---|
| Caso de uso | **Exposição completa de dados pessoais por múltiplos identificadores.** |
| Objetivo | Investigar a exposição de múltiplos dados de uma mesma pessoa, combinando e-mails, telefones, usernames e CPF na busca para ter uma visão completa da exposição de um único indivíduo por vários identificadores. |
| Busca | `user=({{"User123" OR "12345678900" OR "+5511987654321" OR "user@company.com"}})` |

**#62** Times: Blue Team — Contexto: Credenciais

| | |
|---|---|
| Caso de uso | **Vazamento de credenciais em grupos famosos do Telegram.** |
| Objetivo | Investigar o vazamento de credenciais em grupos famosos no Telegram, buscando por credenciais expostas, por exemplo, no grupo 'STARLINK*'. |
| Busca | `messageChatName=STARLINK*` |

**#63** Times: Blue Team — Contexto: Credenciais

| | |
|---|---|
| Caso de uso | **Senhas em texto limpo relacionadas ao domínio corporativo.** |
| Objetivo | Identificar senhas em texto limpo relacionadas ao domínio corporativo da empresa ou de terceiros, listando credenciais da empresa com senhas em texto aberto. |
| Busca | `emailDomain={{company.com}} AND passwordType=PLAIN` |

**#64** Times: Blue Team Contexto: Credenciais

| | |
|---|---|
| Caso de uso | **Credenciais em formato hash associadas à empresa.** |
| Objetivo | Encontrar credenciais com hashes, listando credenciais em HASH associadas à empresa. |
| Busca | `emailDomain={{company.com}} AND passwordType=(MD5 OR SHA1 OR MYSQL323)` |

**#65** Times: Blue Team Contexto: Credenciais

| | |
|---|---|
| Caso de uso | **Exposição de credenciais de colaboradores em vazamentos de fornecedores.** |
| Objetivo | Verificar a exposição de credenciais de colaboradores em vazamentos de fornecedores, buscando por credenciais expostas da sua empresa que possuem endereço de acesso a ferramentas do fornecedor. |
| Busca | `accessUrl={{partner.com}} AND emailDomain={{company.com}}` |

**#66** Times: Blue Team Contexto: Credenciais

| | |
|---|---|
| Caso de uso | **Credenciais corporativas em grandes vazamentos setoriais.** |
| Objetivo | Identificar credenciais corporativas em grande vazamento do setor, buscando credenciais expostas da sua empresa associadas ao arquivo de um determinado grande vazamento. |
| Busca | `fileName="leak.txt" AND emailDomain={{company.com}}` |

**#67** Times: Blue Team Contexto: Credenciais

| | |
|---|---|
| Caso de uso | **Análise de reutilização de senhas em casos de fraude.** |
| Objetivo | Analisar o caso de um cliente que reutilizou senhas e sofreu fraude, buscando credenciais reutilizadas em diferentes plataformas com diferentes nomes de usuário. |
| Busca | `user=({{customer@example.com OR "Username" OR 12345678910}})` |

**#68** Times: Blue Team Contexto: Credenciais

Caso de uso **Tentativas de login múltiplas com credenciais expostas e senhas fracas.**

Objetivo Investigar tentativas de login múltiplas relatadas por um cliente, buscando credenciais expostas com senhas consideradas fracas.

Busca
```
user={{customer@example.com}} AND passwordLength<8 AND passwordHasSpecialCharacter=false
```

**#69** Times: Blue Team Contexto: Credenciais

Caso de uso **Presença da empresa em vazamentos massivos de fóruns clandestinos.**

Objetivo Detectar a presença de sua empresa ou clientes em um vazamento massivo identificado, buscando ocorrências dentro de um arquivo específico citado em fóruns clandestinos.

Busca
```
fileName="Collection1.txt" AND emailDomain="{{company.com}}"
```

**#70** Times: Blue Team Contexto: Credenciais

Caso de uso **Senhas fracas da empresa em vazamentos amplamente divulgados.**

Objetivo Verificar senhas fracas em vazamentos amplamente divulgados, explorando um arquivo específico em busca de senhas vulneráveis associadas à empresa.

Busca
```
fileName="{{COMB2024.txt}}" AND emailDomain="{{company.com}}" AND passwordLength<=8
```

**#71** Times: Blue Team Contexto: Credenciais

Caso de uso **Credencial de colaborador vazada por reutilização de username externo.**

Objetivo Identificar se um colaborador teve a credencial de acesso vazada, buscando por nome de usuário usado externamente e detectando o uso anterior do mesmo username em vazamentos.

Busca
```
user="{{user123}}"
```

#72 Times: Blue Team Contexto: Credenciais

Caso de uso **Presença de CNPJ ou CPF em vazamentos conforme LGPD.**

Objetivo Confirmar a presença de CNPJ ou CPF em vazamentos, buscando por números de identificação de pessoa física ou jurídica que possam configurar dados sensíveis, segundo a LGPD.

Busca `"123456789000012"`

#73 Times: Blue Team Contexto: Credenciais

Caso de uso **Nomes completos expostos em vazamentos públicos.**

Objetivo Investigar o uso indevido de nome completo em vazamentos públicos, buscando exposições com nome textual, o que pode ajudar a encontrar informações relevantes para nomes específicos.

Busca `"John Doe"`

#74 Times: Blue Team Contexto: Credenciais

Caso de uso **Tentativas bloqueadas por autenticação multifator.**

Objetivo Detectar tentativas de acesso barradas por autenticação multifator, buscando por repetições da mesma senha entre diferentes vazamentos, o que é útil para encontrar outros usernames do mesmo usuário quando a senha é bem específica.

Busca `password="password123"`

#75 Times: Blue Team Contexto: Credenciais

Caso de uso **Usuários com acesso privilegiado a APIs internas.**

Objetivo Identificar a exposição de usuários específicos com acesso a APIs internas, buscando por credenciais desses usuários com acesso a sistemas internos ou gerenciadores, e listando acessos críticos com alto risco de privilégio (usuários padrão).

Busca `user=admin AND accessUrl=*api-manager*`

#76 Times: Blue Team Contexto: Credenciais

Caso de uso **Contas administrativas em sistemas legados.**

Objetivo Verificar o vazamento de contas administrativas em sistemas legados, identificando "admin", "root", ou "webmaster" associados a IPs internos ou localhost (usuários padrão).

Busca `user=admin AND (accessUrl=192.168* OR accessUrl=127.0.0.1*)`

#77 Times: Anti-Fraud Team Contexto: Credenciais

Caso de uso **Credenciais comprometidas de aplicativos móveis.**

Objetivo Identificar credenciais que apontam para uso em aplicativos, avaliando credenciais comprometidas que acessam um aplicativo específico e listando credenciais expostas associadas a esse app via Google Play ID.

Busca `accessAppId="{{com.example.app}}"`

#78 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Cartões de crédito vazados de outras instituições.**

Objetivo Mapear fontes de vazamento de cartões recorrentes no setor, buscando por BINs de cartões de outras instituições financeiras vazadas.

Busca `bin=(123456 OR 246810 OR 654321)`

#79 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Cartões da empresa na deep & dark web.**

Objetivo Identificar cartões da empresa circulando na Deep Web, buscando cartões com origem na Deep/Dark Web que estejam possivelmente em comercialização por atores maliciosos.

Busca `sourceName="Deep/Dark Web" AND bin=123456`

#80 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Cartões vazados em grupos do Telegram.**

Objetivo Investigar o vazamento de cartões em um grupo específico do Telegram, buscando por cartões publicados em um famoso grupo do Telegram.

Busca `messageChatName="CHECK CREDIT CARDS | LIVE CARDS"`

#81 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Análise de reembolso por cobrança indevida.**

Objetivo Analisar a solicitação de reembolso de um cliente que alega cobrança indevida, verificando se o cartão do cliente foi vazado recentemente e utilizado na cobrança não autorizada.

Busca `cardNumber=12345678910 AND detectionDate>=2025-05-01`

#82 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Compras não autorizadas em múltiplos cartões.**

Objetivo Investigar compras não autorizadas feitas pelo mesmo indivíduo em cartões distintos, buscando múltiplos cartões vinculados ao mesmo titular.

Busca `holder="John Doe"`

#83 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Dados inseridos em site fraudulento.**

Objetivo Analisar o caso de um cliente enganado que inseriu dados em um site falso, buscando a exposição de cartões de crédito, tendo apenas os números parciais do cartão.

Busca `cardNumber=*3920 AND detectionDate>=2025-05-01`

#84 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Cartões com validade futura ainda ativos.**

Objetivo Verificar riscos em cartões com validade futura ainda ativa, buscando cartões com validade superior ao ano de 2025 que ainda possam ser utilizados de forma fraudulenta.

Busca `expirationYear>=25 AND bin=123456`

#85 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Cartões vazados antes de incidente específico.**

Objetivo Analisar cartões vazados antes de um incidente ocorrido em janeiro de 2025, buscando cartões detectados até 31 de dezembro de 2024 para um determinado BIN.

Busca `detectionDate<=2024-12-31 AND bin=123456`

#86 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Cartões em grandes vazamentos conhecidos.**

Objetivo Identificar cartões comprometidos em grandes vazamentos conhecidos, buscando por números de cartões de crédito em arquivos de grandes vazamentos.

Busca `fileName="History.txt"`

#87 Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso **Cartões com CVV disponível para fraude.**

Objetivo Buscar cartões com CVV disponível, mais vulneráveis a uso fraudulento, filtrando cartões que possuem o campo CVV preenchido para um BIN específico.

Busca `cvv=* AND bin=123456`

**#88** Times: Anti-Fraud Team Contexto: Cartão de Crédito

Caso de uso

**Cartões de executivos em vazamentos.**

Objetivo

Localizar cartões de executivos presentes em vazamentos, filtrando por múltiplos nomes de titulares, para identificar cartões possivelmente relacionados a executivos ou pessoas-chave da organização.

Busca

```
holder=("John Doe" OR "Jane Doe" OR "Michael Scott")
```

**#89** Times: Blue Team, Anti-Fraud Team Contexto: Anúncios & Busca Paga

Caso de uso

**Anúncios que personificam a marca, mas não direcionam para o site oficial.**

Objetivo

Buscar anúncios patrocinados na Meta que façam a personificação de uma marca, mas que não estejam redirecionando para o site oficial da companhia. Casos assim podem ser vetores de propagação de phishings.

Busca

```
impersonatedBrandsHigh={{company}} AND NOT adFinalUrl=*{{company.com.br}}*
```

**#90** Times: Blue Team, Anti-Fraud Team Contexto: Anúncios & Busca Paga

Caso de uso

**IDs de perfis que criam muitos anúncios de fraude.**

Objetivo

Investigar e coletar evidências de que um perfil está disseminando grandes quantidades de fraudes. Muitas vezes os perfis não usam logo da marca, o que dificulta a identificação e remoção.

Busca

```
metaProfileId=12312437816347236
```

**#91** Times: Blue Team, Anti-Fraud Team Contexto: Anúncios & Busca Paga

Caso de uso

**Templates de anúncios comuns.**

Objetivo

Identificar anúncios que usam o mesmo template (collation). Essa informação pode ser útil para identificar padrões dos fraudadores.

Busca

```
collationId=12312437816347236
```

#92 Times: Blue Team, Anti-Fraud Team Contexto: Anúncios & Busca Paga

Caso de uso **Nomes de perfis comuns em fraudes.**

Objetivo Investigar perfis com nomes suspeitos que podem estar criando muitas fraudes.

Busca `metaProfileName="{{Nome do perfil}}"`

#93 Times: Blue Team, Anti-Fraud Team Contexto: Anúncios & Busca Paga

Caso de uso **Esquema de cores da identidade visual da marca.**

Objetivo Buscar por esquemas de cores que identifiquem a identidade visual de uma marca. Em muitos anúncios os fraudadores não usam logotipos, mas usam o esquema de cores para atrair as vítimas.

Busca `predominantColorHex=#FE3131`

#94 Times: Blue Team, Anti-Fraud Team Contexto: Anúncios & Busca Paga

Caso de uso **Utilização do nome da marca na descrição do anúncio.**

Objetivo Buscar pelo nome da marca, ou por expressões específicas frequentemente usadas pelas marcas, como slogans.

Busca `adDescription={{companyName}}`

#95 Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso **Pagina com o favicon.**

Objetivo Buscar por páginas que usam o favicon da companhia, pode-se buscar pelo nome do arquivo ou pelo hash.

Busca

```
resourceFilename="nficon2016.ico"
resourceHash=29dd20bc4b9b45bb7e0898e27af633320c9ae2b3e89d933f7aa6522ba238f171
```

Top Search #96 — Times: Blue Team, Anti-Fraud Team — Contexto: URLs & Domínios

Caso de uso

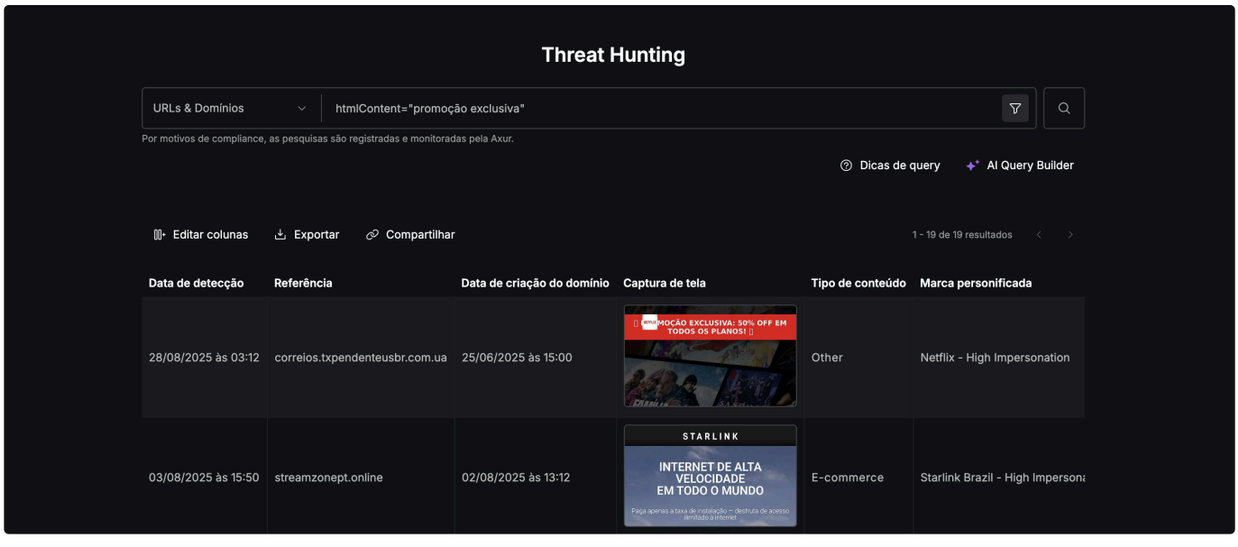
**Texto no HTML.**

Objetivo

Buscar por texto no HTML, como por exemplo frases utilizadas pela sua marca no site oficial, como também identificadores únicos como CNPJ, números de telefone ou endereços.

Busca

```
htmlContent:"promoção exclusiva"
```




#97 — Times: Blue Team, Anti-Fraud Team — Contexto: URLs & Domínios

Caso de uso

**Arquivos com a marca no nome.**

Objetivo

Buscar por nome de arquivos como company_logo.png para encontrar páginas que usam os mesmos artefatos da página original.

Busca

```
resourceFilename=*{{company}}*
```

#98 — Times: Blue Team, Anti-Fraud Team — Contexto: URLs & Domínios

Caso de uso

**Fonte usada por kit phishing.**

Objetivo

Buscar por uma fonte específica, usada por um kit phishing.

Busca

```
resourceFilename="memvYaGs126MiZpBA-UvWbX2vVnXBbObj2OVTS-mu0SC55I.woff2"
```

Top Search 99 Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

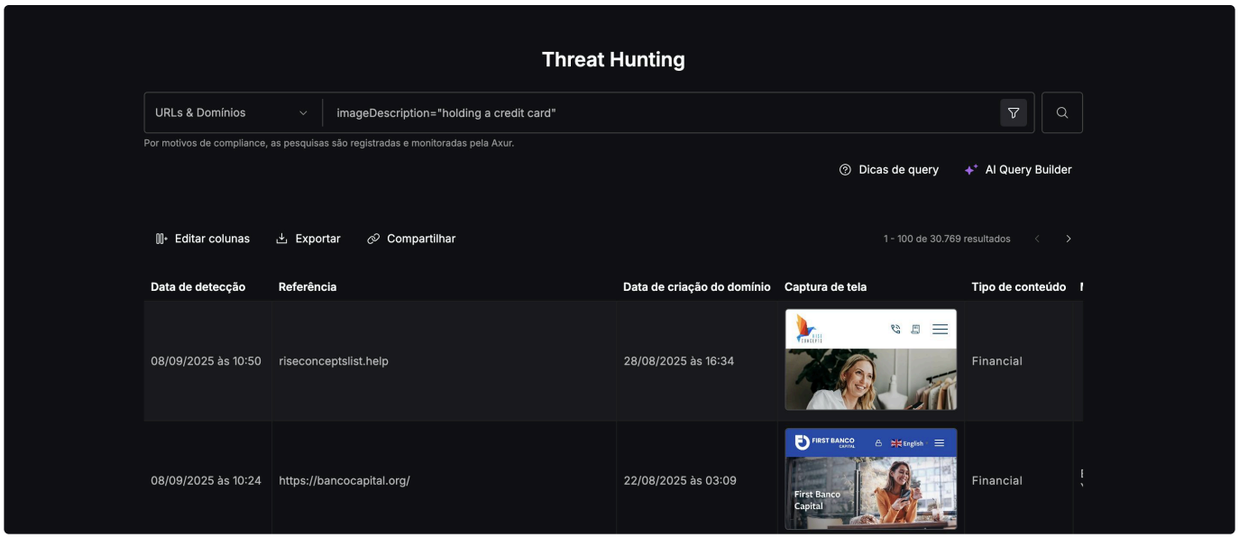
**Descrições de imagem do screenshot.**

Objetivo

Buscar por descrições de imagem do screenshot, usando elementos como "mão segurando cartão de crédito".

Busca

```
imageDescription="holding a credit card"
```




#100 Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Não tem portas abertas.**

Objetivo

Buscar por domínios recentemente criados, mas que ainda não tem portas 80 e 443 abertas.

Busca

```
domainCreationDate>=2025-08-01 AND NOT _exists_:ports AND reference={{company}}~1
```

#101 Times: Blue Team, Anti-Fraud Team Contexto: URLs & Domínios

Caso de uso

**Termos em URLs finais de redirecionamento.**

Objetivo

Buscar por termos específicos comuns em Kits de phishing que aparecem apenas em URLs finais de redirecionamento.

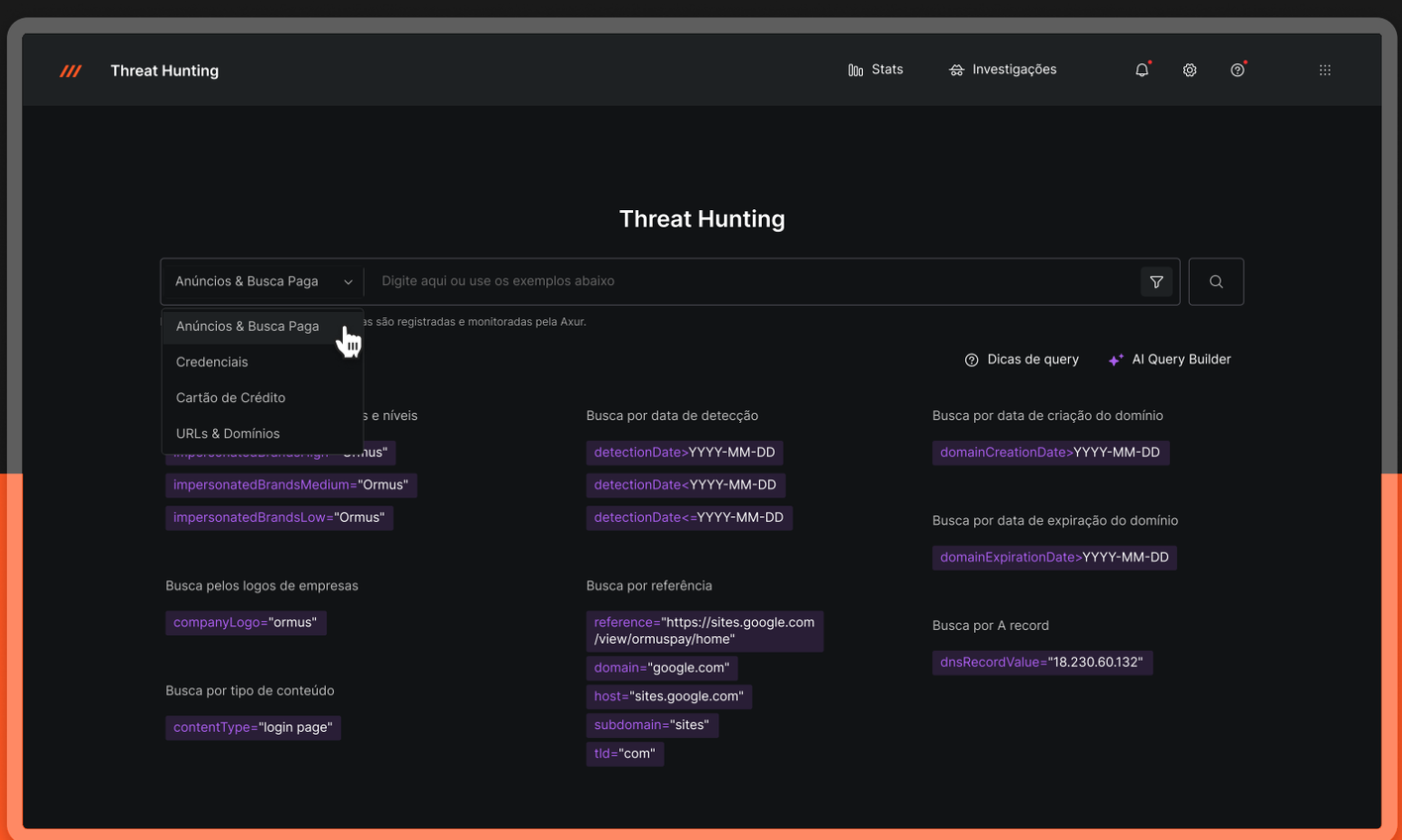
Busca

```
impersonatedBrandsHigh={{company}} AND (redirectedTo=produto OR redirectedTo=checkout)
```

# Experimente o Threat Hunting

Os 101 casos de uso do Threat Hunting da Axur mostram que a detecção de ameaças externas não é um exercício pontual, mas uma prática contínua para reduzir riscos que se estende à várias áreas da organização.

Cada caso evidencia como credenciais, ativos digitais e informações expostas podem ser explorados de formas diferentes, e como a antecipação faz diferença na resposta. O aprendizado é claro: quanto maior a visibilidade sobre o que circula fora dos seus sistemas, maior a capacidade de proteger negócios de forma eficaz.




## Ganhe acesso à uma das maiores bases de dados de ameaças do mundo.

FAÇA UMA DEMO

ISO/IEC 27001 Information Security Management CERTIFIED

Gartner Peer Insights 4.9

Conheça todas as nossas soluções: **axur.com**

AXUR