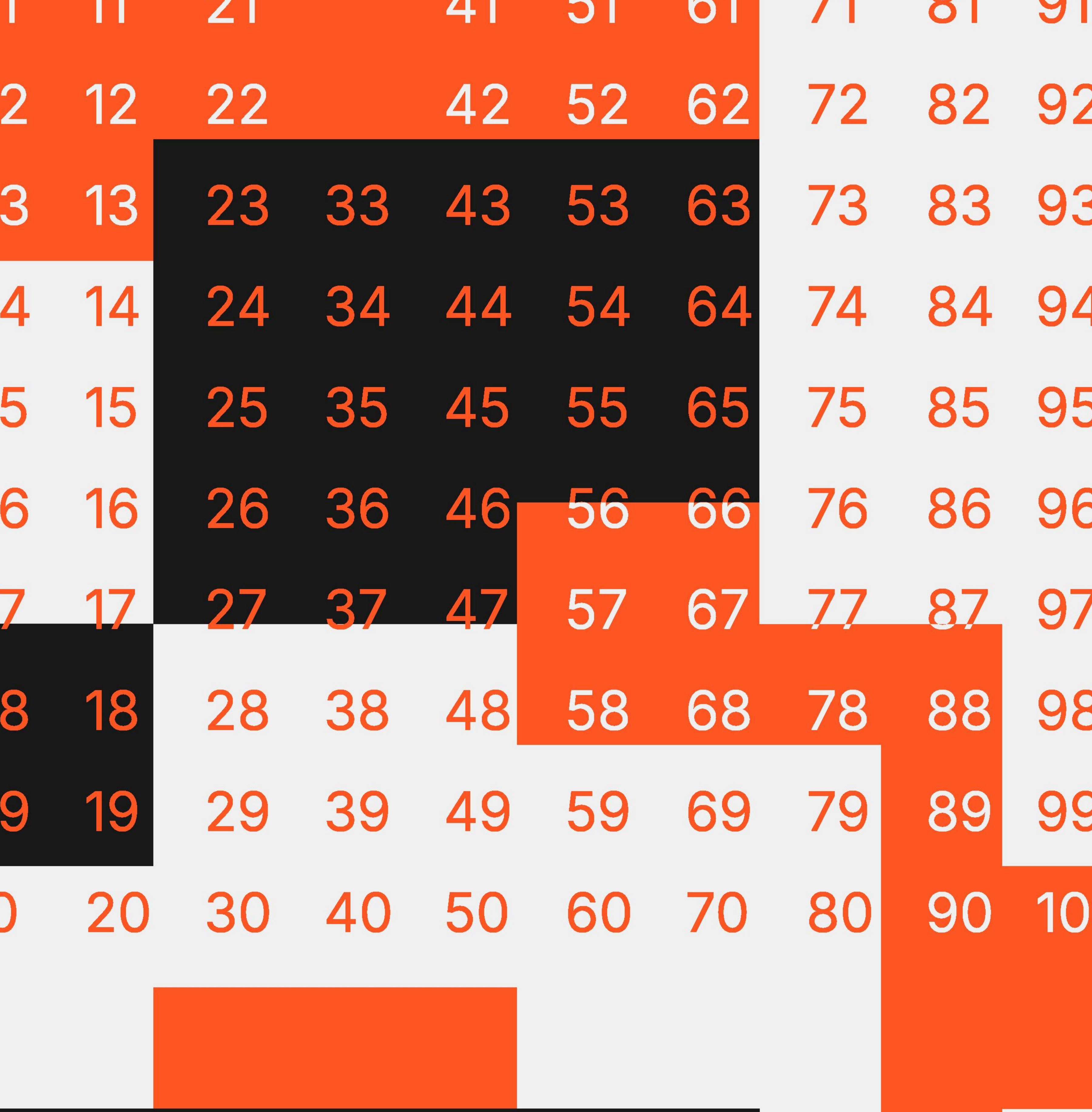


AXUR

101 Threat Hunting Use Cases

Table of Contents

Real-World Use Cases, Immediate Results

Threat Hunting is an advanced investigation capability within the Axur platform. It allows users to search across a vast threat intelligence database using credentials, credit cards, ads, URLs, and domains. To help you extract maximum value from the tool, we've compiled real-world use cases that show how our customers and partners are leveraging the solution.

These are 101 practical ways to search for threats and drive results in your investigations.

With Threat Hunting, you can uncover threats and incidents both inside and outside your monitored assets, taking full advantage of the industry's largest malicious data lake. Backed by an AI model that detects threats visually and contextually in any language, the platform enriches and prioritizes every signal for faster response.

- Strategic Use Cases
- Threat and Incident Response
- Deep Investigations to Mitigate Risk

★ Top Search **#01**

Teams: Blue Team, Anti-Fraud Team

Context: URLs & Domains

Use case

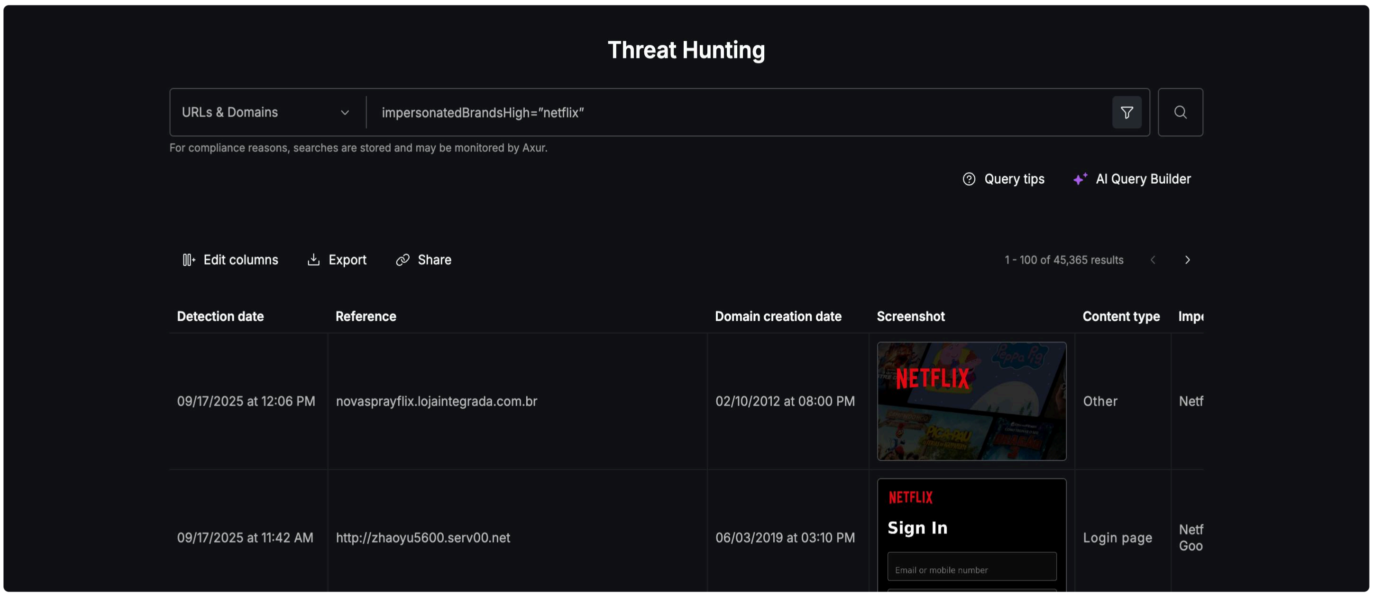
Identification of campaigns with a high level of visual and textual impersonation of the company's identity.

Goal

Identify campaigns with strong impersonation, focusing on domains closely tied to the brand and pages that clearly simulate the company's identity.

Query

```
impersonatedBrandsHigh=”{{company}}”
```



Threat Hunting

URLs & Domains | impersonatedBrandsHigh="netflix"

For compliance reasons, searches are stored and may be monitored by Axur.

1 - 100 of 45,365 results

Detection date	Reference	Domain creation date	Screenshot	Content type	Impe
09/17/2025 at 12:06 PM	novasprayflix.lojaintegrada.com.br	02/10/2012 at 08:00 PM	NETFLIX	Other	Netf
09/17/2025 at 11:42 AM	http://zhaoyu5600.serv00.net	06/03/2019 at 03:10 PM	NETFLIX Sign In Email or mobile number	Login page	Netf Goo

#02

Teams: Blue Team, Anti-Fraud Team

Context: URLs & Domains

Use case

Detection of seasonal (and competitor-related) campaigns through holiday-themed pages.

Goal

Identify broad seasonal campaigns in the industry by searching for pages related to holidays. As a variation, you can include competitors in the filter. For example: `impersonatedBrandsHigh="amazon"`.

Query

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

#03

Teams: Blue Team, Anti-Fraud Team

Context: URLs & Domains

Use case

Recently registered malicious URLs in the financial sector (adaptable to other industries).

Goal

Identify newly registered malicious URLs in the financial sector, with flexibility to apply the same logic to other industries as needed.

Query

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

#04 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case **Detection of popular TLDs in financial and e-commerce scams.**

Goal Identify domains using popular TLDs in financial and e-commerce scams, such as .shop, to uncover threats on fake online store sites.

Query

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

#05 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case **Financial phishing threats using payment-related domains.**

Goal Detect financial phishing campaigns that leverage payment-themed TLDs, such as .pay, to impersonate payment pages.

Query

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

#06 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case **Domains reserved for future campaigns but currently inactive.**

Goal Identify domains reserved as preparation for future campaigns by searching for those registered in the last 90 days that remain inactive, contain no content, or are flagged as “parked.”

Query

```
contentType=("blank page" OR "parked domain") AND reference={{company}}~1
AND NOT domain={{company.com}} AND domainCreationDate>2025-06-30
```

#07 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case **Domains returning error pages as part of “on/off” phishing attacks.**

Goal Detect domains that return error pages and may be used in “on/off” phishing schemes, where fake sites are switched on and off at specific times.

Query

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

#08 Teams: Legal, Compliance Context URLs & Domains

Use case	**Domains related to gambling activities that misuse the company's brand.**
Goal	Identify domains tied to gambling activity that use or associate the company brand, focusing on content classified as "gambling" where the brand is explicitly mentioned.
Query	`contentType="gambling" AND companiesMentioned={{company}}`

#09 Teams: Legal, Compliance Context: URLs & Domains

Use case	**Domains posing as news sources for disinformation.**
Goal	Investigate domains that appear to be news outlets by searching for content classified as "news" where the company is mentioned in the HTML or images. These sites may imitate major news portals to spread disinformation or manipulation. As a variation, you can search specifically for the use of the company's logo, e.g., `companyLogo="company"`.
Query	`contentType="news" AND companiesMentioned={{company}}`

#10 Teams: Blue Team, Anti-Fraud Team Context URLs & Domains

Use case	**Fake financial pages imitating banks and fintechs.**
Goal	Detect fake financial pages that mimic legitimate institutions. This can be applied to a specific company or to the broader financial sector. The query can target content classified as "financial," identifying pages impersonating banks, fintechs, or card issuers.
Query	`contentType="financial" AND impersonatedBrand={{company}}`

#11 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case	**Fake login pages designed to steal credentials.**
Goal	Identify fraudulent login pages created to harvest credentials by searching for content classified as "login page."
Query	`contentType="login page" AND impersonatedBrand={{company}}`

#12 Teams: Legal, Compliance Context: URLs & Domains

Use case

Fake e-commerce scams with non-existent products.

Goal

Identify scams using fraudulent e-commerce pages with non-existent or cloned products. Focus on content classified as “e-commerce” that mentions the company and is hosted on domains registered within the last 90 days.

Query

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

#13 Teams: Legal, Compliance Context URLs & Domains

Use case

Adult content pages associated with the company’s brand.

Goal

Detect pages containing adult content that associate with or misuse the company’s brand by searching for content classified as “adult” where the company is mentioned.

Query

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

#14 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case

Domains and hosts using the exact brand name.

Goal

Identify domains and hosts that directly use the company’s brand name by searching for its exact presence in the domain or host.

Query

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

#15 Teams: Blue Team Context: URLs & Domains

Use case

Phishing campaigns operated from the same geographic region.

Goal

Map phishing campaigns operated from a single geographic region by using geolocation data to identify clusters of attacks targeting the company, hosted on specific ISPs, for example, in Russia.

Query

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

Top Search #16

Teams: Blue Team, Anti-Fraud Team

Context: URLs & Domains

Use case

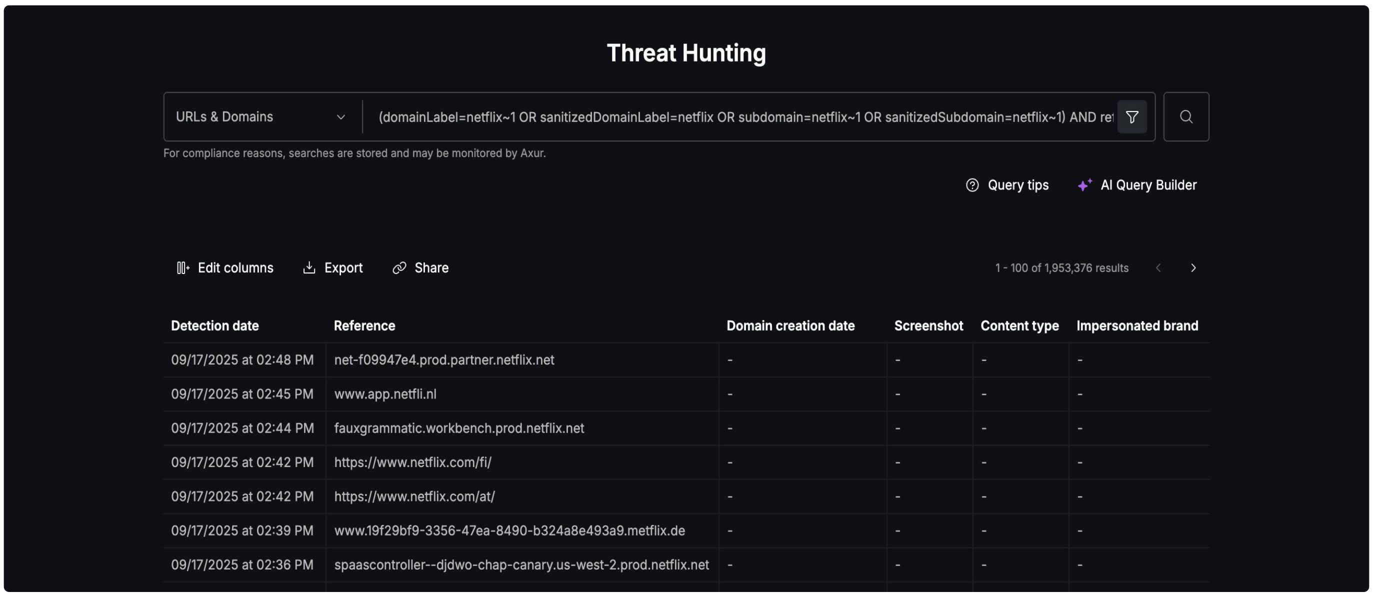
Domains and hosts similar to the brand with variations and homoglyphs.

Goal

Identify domains and hosts resembling the brand by searching for variations of the brand name in domains, including typos and homoglyph attacks.

Query

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



Threat Hunting

URLs & Domains | (domainLabel=netflix~1 OR sanitizedDomainLabel=netflix OR subdomain=netflix~1 OR sanitizedSubdomain=netflix~1) AND ref

For compliance reasons, searches are stored and may be monitored by Axur.

1 - 100 of 1,953,376 results

Detection date	Reference	Domain creation date	Screenshot	Content type	Impersonated brand
09/17/2025 at 02:48 PM	net-f09947e4.prod.partner.netflix.net	-	-	-	-
09/17/2025 at 02:45 PM	www.app.netfli.nl	-	-	-	-
09/17/2025 at 02:44 PM	fauxgrammatic.workbench.prod.netflix.net	-	-	-	-
09/17/2025 at 02:42 PM	https://www.netflix.com/fi/	-	-	-	-
09/17/2025 at 02:42 PM	https://www.netflix.com/at/	-	-	-	-
09/17/2025 at 02:39 PM	www.19f29bf9-3356-47ea-8490-b324a8e493a9.metflix.de	-	-	-	-
09/17/2025 at 02:36 PM	spaascontroller--djdwo-chap-canary.us-west-2.prod.netflix.net	-	-	-	-

#17

Teams: Blue Team

Context: URLs & Domains

Use case

Phishing campaigns operated from the same geographic region.

Goal

Map phishing campaigns originating from a single geographic region by using geolocation data to identify clusters of attacks. For example, fake Microsoft and Apple login pages hosted on ISPs in Russia.

Query

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

#18

Teams: Blue Team

Context: URLs & Domains

Use case

Phishing campaigns using the same ISP.

Goal

Investigate phishing campaigns hosted on the same ISP by identifying fraudulent pages that share the same hosting infrastructure.

Query

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

★ Top Search #19

Teams: Blue Team, Anti-Fraud Team

Context: URLs & Domains

Use case

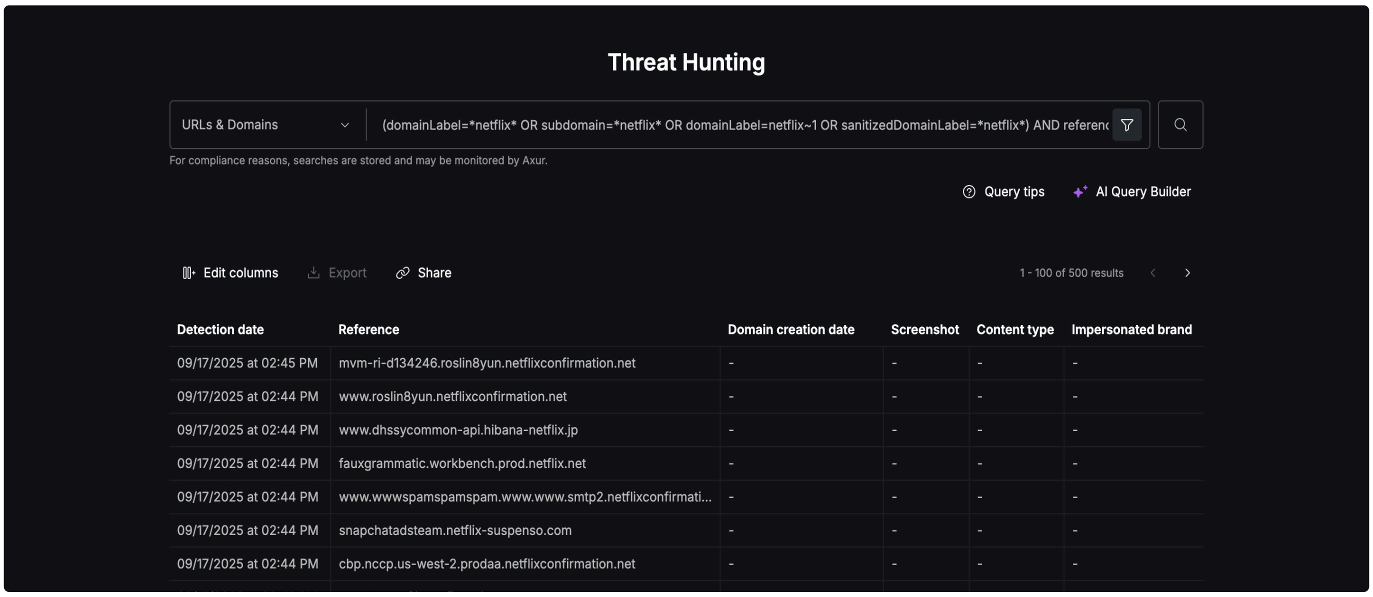
Broad search for similar domains with high detection volume.

Goal

Identify domains and hosts similar to the brand by searching for the brand name in any part of the domain, including variations such as typos and homoglyphs. Depending on the brand, this type of query may generate a very large number of detections.

Query

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



Threat Hunting

URLs & Domains | (domainLabel=*netflix* OR subdomain=*netflix* OR domainLabel=netflix~1 OR sanitizedDomainLabel=*netflix*) AND referenc

For compliance reasons, searches are stored and may be monitored by Axur.

1 - 100 of 500 results

Detection date	Reference	Domain creation date	Screenshot	Content type	Impersonated brand
09/17/2025 at 02:45 PM	mvm-ri-d134246.roslin8yun.netflixconfirmation.net	-	-	-	-
09/17/2025 at 02:44 PM	www.roslin8yun.netflixconfirmation.net	-	-	-	-
09/17/2025 at 02:44 PM	www.dhssycommon-api.hibana-netflix.jp	-	-	-	-
09/17/2025 at 02:44 PM	fauxgrammatic.workbench.prod.netflix.net	-	-	-	-
09/17/2025 at 02:44 PM	www.wwwspamspamspam.www.www.smtp2.netflixconfirmati...	-	-	-	-
09/17/2025 at 02:44 PM	snapchatadsteam.netflix-suspenso.com	-	-	-	-
09/17/2025 at 02:44 PM	cbp.nccp.us-west-2.prodaa.netflixconfirmation.net	-	-	-	-

#20

Teams: Blue Team

Context: URLs & Domains

Use case

Pages requesting payment data associated with the brand.

Goal

Analyze pages that request payment information while impersonating the brand. The focus is on pages with payment forms linked to the company or its industry.

Query

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

#21

Teams: Blue Team

Context: URLs & Domains

Use case

URLs leveraging Visa, Mastercard, and the company's brand.

Goal

Investigate URLs that use Visa, Mastercard, and the company brand together by identifying pages where Visa or Mastercard are mentioned alongside the company's brand.

Query

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

#22 Teams: Blue Team Context:: URLs & Domains

Use case

Validation of suspicious URLs across multiple specialized databases.

Goal

Validate whether a suspicious URL is listed in multiple phishing intelligence sources, confirming if the domain has already been flagged as malicious and ensuring broader coverage.

Query

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

#23 Teams: Blue Team, Anti-Fraud Team Context:: URLs & Domains

Use case

Malicious pages promoted via Facebook Ads campaigns.

Goal

Investigate malicious pages promoted through paid Facebook Ads by identifying fake sponsored URLs impersonating the brand and consolidating a list of these advertised threats.

Query

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

#24 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case

Campaigns linked to the same profile after a fraud detection.

Goal

Track campaigns tied to the same profile after detecting fraud through Facebook Ads, mapping the history of fraudulent campaigns operated by the same actor.

Query

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

#25 Teams: Blue Team, Anti-Fraud Team Context:: URLs & Domains

Use case

Frauds promoted by the same advertiser link after a deceptive campaign.

Goal

Identify frauds promoted by the same advertiser link following a deceptive campaign, tracing additional campaigns associated with the same URL and consolidating a list of fraudulent activity tied to that advertiser profile.

Query

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

★ Top Search **#26** Teams: Blue Team, Anti-Fraud Team, Legal, Compliance Context: URLs & Domains

Use case

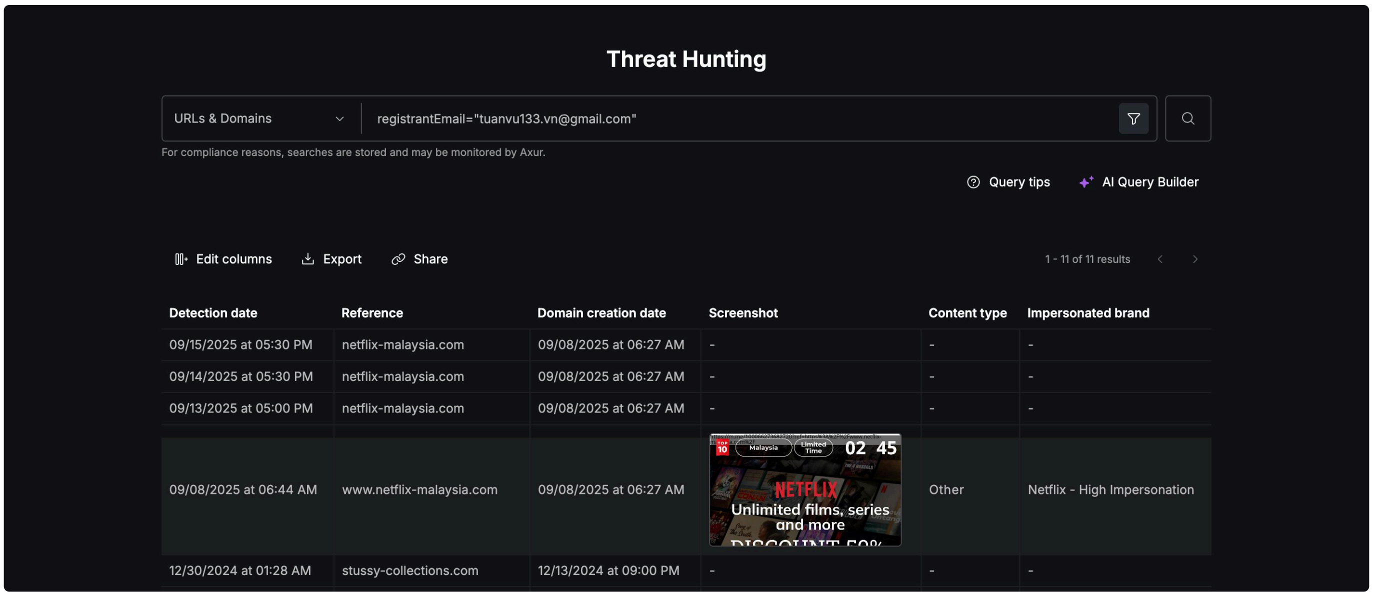
Malicious pages tied to the same registrant or registration email.

Goal

Investigate malicious pages associated with the same registrant or WHOIS registration email, tracking fraud campaigns that reuse registration data and identifying potential fraudulent pages created by the same registrant.

Query

```
registrantEmail="{{fraudster@mail.com}}"
```



Threat Hunting

URLs & Domains | registrantEmail="tuanvu133.vn@gmail.com"

For compliance reasons, searches are stored and may be monitored by Axur.

Detection date	Reference	Domain creation date	Screenshot	Content type	Impersonated brand
09/15/2025 at 05:30 PM	netflix-malaysia.com	09/08/2025 at 06:27 AM	-	-	-
09/14/2025 at 05:30 PM	netflix-malaysia.com	09/08/2025 at 06:27 AM	-	-	-
09/13/2025 at 05:00 PM	netflix-malaysia.com	09/08/2025 at 06:27 AM	-	-	-
09/08/2025 at 06:44 AM	www.netflix-malaysia.com	09/08/2025 at 06:27 AM		Other	Netflix - High Impersonation
12/30/2024 at 01:28 AM	stussy-collections.com	12/13/2024 at 09:00 PM	-	-	-

#27 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case

Recent campaigns hosted by providers like Cloudflare.

Goal

Investigate recent phishing or fraud campaigns hosted by providers such as Cloudflare by correlating threats that use the same hosting infrastructure and identifying newly registered malicious domains tied to the same ISP.

Query

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

#28 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case

Campaigns sharing the same DNS infrastructure.

Goal

Investigate campaigns that rely on the same DNS infrastructure by hunting for domains connected to past campaigns using the same name servers, identifying potential fraud through DNS reuse.

Query

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

#29 Teams: Blue Team Context: URLs & Domains

Use case

Pages potentially used to harvest corporate credentials.

Goal

Identify pages that could be used to capture corporate credentials by searching for fake Google and Microsoft login pages hosted on domains mentioning the client’s brand. The purpose is to detect phishing campaigns targeting employees to steal corporate access credentials.

Query

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

#30 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case

Domains potentially used for spear phishing without an active web page.

Goal

Identify domains that could be leveraged for spear phishing by searching for domains impersonating the company’s brand that have MX records configured for email sending but lack an active website.

Query

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

#31 Teams: Legal, Compliance Context: URLs & Domains

Use case

Association of the brand (logo) with inappropriate content such as gambling.

Goal

Detect brand association with inappropriate content, such as gambling, by searching for pages classified as “gambling” that display the company’s logo.

Query

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

#32 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Pages potentially used for fraud in other countries.

Goal

Identify pages potentially used for fraud in foreign regions by searching for pages impersonating the brand in languages other than English and in geographies where the company does not operate.

Query

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

#33 Teams: Blue Team Context: URLs & Domains

Use case

Malicious content hosted on inactive company subdomains.

Goal

Discover malicious content hosted on company-owned subdomains that should be inactive by investigating cases of subdomain hijacking. The analysis should generate a list of company subdomains configured with CNAME records pointing to third-party hosting providers, helping to identify which are vulnerable or being misused.

Query

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

#34 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Detection of domains exclusively using IPv6 with AAAA records to evade monitoring.

Goal

Identify domains that use only IPv6 and reference the company by searching for domains with AAAA records but no A records. Exclusive IPv6 usage may indicate intentional configuration to avoid detection, since some tools and firewalls still provide limited IPv6 coverage.

Query

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

#35 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Pages misusing the company logo without textual reference in the domain.

Goal

Identify pages that display the company logo without mentioning the brand name in the URL, detecting misuse of visual elements with no textual reference in the domain.

Query

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

#36 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Recently registered domains (within 60 days) using the brand.

Goal

Identify domains registered in the past 60 days that host pages impersonating the brand or using its name.

Query

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

★ Top Search #37 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domains

Use case

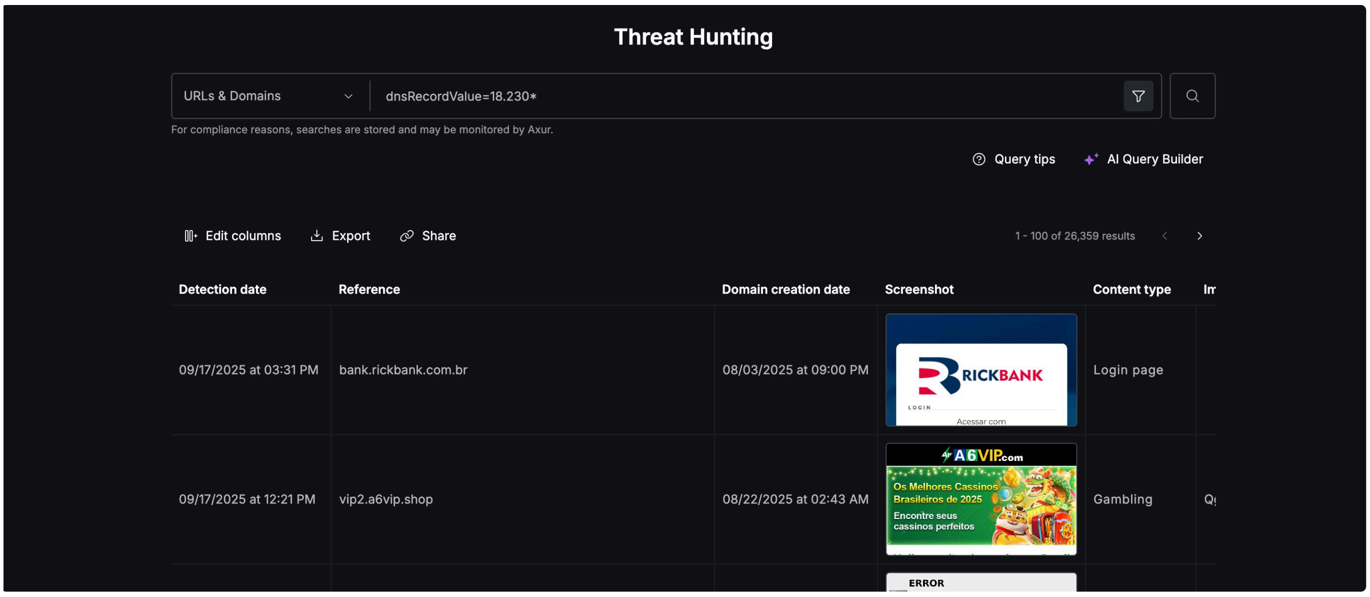
Campaigns sharing the same IP block.

Goal

Investigate campaigns that share the same IP block (prefixes or octets). Starting from one identified phishing page, expand the search to uncover other pages hosted on the same infrastructure.

Query

```
dnsRecordValue=18.230*
```



Threat Hunting

URLs & Domains | dnsRecordValue=18.230*

For compliance reasons, searches are stored and may be monitored by Axur.

1 - 100 of 26,359 results

Detection date	Reference	Domain creation date	Screenshot	Content type	Im
09/17/2025 at 03:31 PM	bank.rickbank.com.br	08/03/2025 at 09:00 PM		Login page	
09/17/2025 at 12:21 PM	vip2.a6vip.shop	08/22/2025 at 02:43 AM		Gambling	Q

RICKBANK
LOGIN
Acessar com
A6VIP.com
Os Melhores Cassinos Brasileiros de 2025
Encontre seus cassinos perfeitos
ERROR

#38 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Misuse of executive names to promote unauthorized products or services.

Goal

Detect unauthorized use of executive names outside legitimate journalistic contexts by searching for pages exploiting their identities to promote products or services.

Query

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

#39 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Fake sites impersonating the company’s technical support to steal personal data.

Goal

Investigate cases where customers reported entering personal data into fake websites impersonating the company’s technical support. Focus on pages that mention the brand, request passwords, and simulate customer assistance, often containing terms like “help” or “customer” in the URL.

Query

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

#40

Teams: Blue Team, Anti-Fraud Team

Context: URLs & Domains

Use case

Fake competitor pages (especially login pages) → anticipate attacks.

Goal

Identify phishing pages targeting competitors in order to anticipate threats. Focus on highly impersonated brand pages registered within the last 90 days. As a more specific variation, you can filter only pages where `contentType="login page"`, prioritizing those that mimic competitors' authentication portals.

Query

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

#41

Teams: Anti-Fraud Team

Context: URLs & Domains

Use case

Identification of campaigns using partial brand elements with medium-level impersonation.

Goal

Identify campaigns that use partial brand elements, targeting fraud cases with medium impersonation. While this query may generate more results, it is useful for detecting outliers or less obvious fraud attempts.

Query

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

#42

Teams: Anti-Fraud Team

Context: URLs & Domains

Use case

Detection of early-stage or subtle campaigns with low-level impersonation of the brand.

Goal

Detect early or subtle impersonation attempts of the brand. Although this query may return a larger volume of results, it helps uncover emerging threats or atypical cases.

Query

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

#43

Teams: Anti-Fraud Team

Context: URLs & Domains

Use case

Identification of pages mentioning the company on sites classified as "financial."

Goal

Identify pages that reference the company, textually or visually, within sites classified as financial.

Query

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

#44 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Verification of the company logo usage on potentially malicious domains classified as “financial.”

Objetivo

Verify the misuse of the company logo on potentially malicious domains by searching for visual brand elements on sites classified as financial.

Query

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

#45 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Tracking visual simulations of apps mentioning the company’s brand.

Objetivo

Track app-like visual simulations by searching for pages designed to look like mobile apps that reference the company’s brand.

Query

```
imageDescription=({{company}} AND "mobile app")
```

#46 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Detection of domains with Telegram links mentioning the company’s brand.

Objetivo

Detect domains containing Telegram links that mention the company by searching for pages referencing the brand with external HTML links pointing to Telegram groups or profiles.

Query

```
htmlLinks=t.me AND companiesMentioned="{{company}}"
```

#47 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Identification of pages redirecting to WhatsApp numbers or groups for scams.

Objetivo

Identify pages redirecting users to WhatsApp numbers or groups to detect scams carried out via direct contact on the platform. This search produces a list of pages encouraging communication with fraudsters through WhatsApp.

Query

```
impersonatedBrandsHigh="{{company}}" AND htmlLinks=wa.me
```

#48

Teams: Anti-Fraud Team

Context: URLs & Domains

Use case

Investigation of fraud schemes organized on Discord servers or groups with HTML links.

Goal

Investigate fraud operations organized through Discord servers or groups by identifying pages containing HTML links that reference the platform. The goal is to detect illegitimate campaigns or communities operating via Discord.

Query

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

#49

Teams: Anti-Fraud Team

Context: URLs & Domains

Use case

Identification of frauds redirecting victims to WhatsApp numbers and tracking related campaigns.

Goal

Identify scams redirecting victims to WhatsApp numbers and, once a fraudulent number is detected, trace other pages tied to the same criminal campaign.

Query

```
htmlLinks=*11922331092*
```

#50

Teams: Anti-Fraud Team

Context: URLs & Domains

Use case

Active malicious domains impersonating the brand, especially recent and operational ones.

Goal

Identify active malicious domains impersonating the brand, with a focus on recently created domains that remain operational and have not yet been suspended.

Query

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

#51

Teams: Anti-Fraud Team

Context: URLs & Domains

Use case

Pages using URL shorteners to mask attacks referencing the brand.

Goal

Detect pages leveraging URL shorteners (e.g., Bit.ly, TinyURL, t.co) to disguise final destinations while referencing the brand, listing the shortened URLs used as attack vectors.

Query

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

#52 Teams: Anti-Fraud Team Context: URLs & Domains

Use case

Phishing attempts with company lookalike domains using the “fuzzy” operator.

Goal

Identify potential phishing attempts by searching for domains similar to the company name (using the fuzzy operator), generating a list of domains resembling company.com that could be used to deceive users.

Query

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

#53 Teams: Blue Team Context: Credentials

Use case

Credential harvesting tactics in the sector and leaked credentials from specific websites.

Goal

Map common credential harvesting tactics in the industry and identify leaked access credentials tied to a specific website, using either the domain or the full URL.

Query

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

#54 Teams: Red & Blue Teams, Legal Context: Credentials

Use case

Vendor security risk through exposed employee credentials.

Goal

Evaluate the security risk of engaging a vendor by searching for exposures of its employees’ credentials.

Query

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

#55 Teams: Red & Blue Teams Context: Credentials

Use case

Prior employee exposure in high-risk sources and the deep and dark web.

Goal

Identify whether an employee has been previously exposed in high-risk sources by searching for leaks related to a specific user and determining the origin, potentially in the deep and dark web.

Query

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

#56 Teams: Blue Team Context: Credentials

Use case

Leaked credentials with a testable access URL.

Goal

Verify whether a leaked credential includes an available access URL by searching for exposed company credentials tied to a login URL that can be immediately tested.

Query

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

#57 Teams: Blue Team Context: Credentials

Use case

Leaked credentials within a specific file.

Goal

Explore large credential dump files for sale in forums and, from there, assess what other credentials originate from the same file to understand its contents, victim profile, and possible connections.

Query

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

#58 Teams: Blue Team, Legal Context: Credentials

Use case

Risk analysis of strategic partners in external leaks.

Goal

Investigate exposures of strategic partners in external leaks, assessing the indirect impact of structured data breaches on those partners to map third-party association risks.

Query

```
fileName="leaked_suppliers.txt" AND content.text="{{vendor.com}}"
```

#59 Teams: Blue Team Context: Credentials

Use case

Exposure of corporate credentials through professional email.

Goal

Check whether a corporate credential has been exposed by searching for all leaked records tied to a specific professional email address.

Query

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

#60 Teams: Anti-Fraud Team, Blue Team Context: Credentials

Use case

Presence of phone numbers in leaks with associated credentials.

Goal

Verify whether a customer's phone number appears in leaks by searching for phone identifiers tied to usernames and checking if credentials are associated, highly relevant in fraud and investigation processes.

Query

```
user="+5511987654321" AND userType="PHONE"
```

#61 Teams: Blue Team Context: Credentials

Use case

Full exposure of personal data across multiple identifiers.

Goal

Investigate the exposure of multiple data points for the same individual by combining email addresses, phone numbers, usernames, and national ID numbers in the search to gain a comprehensive view of a single person's exposure.

Query

```
user=("user123" OR "12345678900" OR "+5511987654321" OR "user@company.com")
```

#62 Teams: Blue Team Context: Credentials

Use case

Credential leaks in well-known Telegram groups.

Goal

Investigate credential leaks shared in well-known Telegram groups, such as exposed credentials posted in the STARLINK group.

Query

```
messageChatName=STARLINK*
```

#63 Teams: Blue Team Context: Credentials

Use case

Plaintext passwords related to the corporate domain.

Goal

Identify plaintext passwords tied to the company's corporate domain, or third parties, by listing credentials associated with the domain where passwords are stored in plain text.

Query

```
emailDomain={{company.com}} AND passwordType=PLAIN
```

#64 Teams: Blue Team Context: Credentials

Use case

Hashed credentials associated with the company.

Goal

Find credentials stored as hashes by listing leaked records associated with the company where the password type is HASH.

Query

```
emailDomain={{company.com}} AND passwordType=(MD5 OR SHA1 OR MYSQL323)
```

#65 Teams: Blue Team Context: Credentials

Use case

Exposure of employee credentials in supplier breaches.

Goal

Verify exposure of employee credentials in supplier-related breaches by searching for leaked company credentials tied to access URLs of supplier tools.

Query

```
accessUrl={{partner.com}} AND emailDomain={{company.com}}
```

#66 Teams: Blue Team Context: Credentials

Use case

Corporate credentials in large-scale sector breaches.

Goal

Identify company credentials exposed in major industry-wide breaches by searching for leaked credentials linked to a specific breach file.

Query

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

#67 Teams: Blue Team Context: Credentials

Use case

Password reuse analysis in fraud cases.

Goal

Investigate cases where a customer reused passwords and suffered fraud by searching for credentials reused across multiple platforms with different usernames.

Query

```
user=(customer@example.com OR "Username" OR 12345678910)
```

#68 Teams: Blue Team Context: Credentials

Use case

Multiple login attempts with exposed credentials and weak passwords.

Goal

Investigate multiple login attempts reported by a customer by searching for exposed credentials with weak passwords.

Query

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

#69 Teams: Blue Team Context: Credentials

Use case

Company presence in massive leaks from underground forums.

Goal

Detect the presence of the company or its customers in a massive leak by searching for occurrences within a specific file shared in underground forums.

Query

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

#70 Teams: Blue Team Context: Credentials

Use case

Weak company passwords in widely publicized leaks.

Goal

Check for weak passwords in widely publicized leaks by exploring a specific file for vulnerable credentials associated with the company.

Query

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

#71 Teams: Blue Team Context: Credentials

Use case

Employee credential leak due to external username reuse.

Goal

Identify whether an employee’s access credential was leaked by searching for usernames reused externally and detecting prior use of the same username in breaches.

Query

```
user="user123"
```

#72 Teams: Blue Team Context: Credentials

Use case

Presence of employee IDs in leaks.

Goal

Confirm whether employee IDs appear in data leaks by searching for exposed records containing internal workforce identifiers, which could indicate compromised access credentials or sensitive HR-related information.

Query

```
"EMP123456"
```

#73 Teams: Blue Team Context: Credentials

Use case

Full names exposed in public leaks.

Goal

Investigate the misuse of full names in public leaks by searching for exposures containing full-text names—helpful for identifying relevant information tied to specific individuals.

Query

```
"John Doe"
```

#74 Teams: Blue Team Context: Credentials

Use case

Blocked login attempts due to multi-factor authentication.

Goal

Detect access attempts blocked by multi-factor authentication by searching for repeated use of the same password across different leaks. This helps identify other usernames linked to the same user when the password is highly specific.

Query

```
password="password123"
```

#75 Teams: Blue Team Context: Credentials

Use case

Users with privileged access to internal APIs.

Goal

Identify exposures of specific users with privileged access to internal APIs by searching for credentials tied to internal systems or managers, listing critical accounts with elevated privilege risk (e.g., default admin users).

Query

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

#76 Teams: Blue Team Context: Credentials

Use case

Administrative accounts in legacy systems.

Goal

Check for leaks of administrative accounts in legacy systems by identifying usernames like admin, root, or webmaster associated with internal IPs or localhost (default accounts).

Query

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

#77 Teams: Anti-Fraud Team Context: Credentials

Use case

Compromised credentials from mobile applications.

Goal

Identify leaked credentials tied to mobile apps by assessing compromised logins connected to a specific application and listing exposed credentials associated with that app via its Google Play ID.

Query

```
accessAppId="com.example.app"
```

#78 Teams: Anti-Fraud Team Context: Credit cards

Use case

Leaked credit cards from other institutions.

Goal

Map recurring sources of credit card leaks in the sector by searching for BINs of cards belonging to other financial institutions.

Query

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

#79 Teams: Anti-Fraud Team Context: Credit cards

Use case

Company-issued cards found in the deep & dark web.

Goal

Identify company-issued credit cards circulating on the Deep or Dark Web by searching for records with that origin, potentially being sold by malicious actors.

Query

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

#80 Teams: Anti-Fraud Team Context: Credit cards

Use case

Leaked credit cards in Telegram groups.

Goal

Investigate the leakage of credit card data in a specific Telegram group by searching for cards posted in well-known underground communities.

Query

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

#81 Teams: Anti-Fraud Team Context: Credit cards

Use case

Chargeback analysis for disputed transactions.

Goal

Analyze a customer's chargeback request due to an alleged unauthorized charge by verifying whether the customer's card was recently leaked and used in fraudulent activity.

Query

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

#82 Teams: Anti-Fraud Team Context: Credit cards

Use case

Unauthorized purchases across multiple cards.

Goal

Investigate unauthorized purchases made by the same individual using different cards by searching for multiple cards tied to the same holder.

Query

```
holder="John Doe"
```

#83 Teams: Anti-Fraud Team Context: Credit cards

Use case

Customer data submitted on a fraudulent website.

Goal

Investigate a case where a customer was deceived into entering card details on a fake website by searching for exposed credit cards using only partial card numbers.

Query

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

#84 Teams: Anti-Fraud Team Context: Credit cards

Use case

Cards with future expiration dates still active.

Goal

Assess risks from cards with valid expiration dates in the future by searching for cards expiring beyond 2025 that could still be used fraudulently.

Query

```
expirationYear>=25 AND bin=123456
```

#85 Teams: Anti-Fraud Team Context: Credit cards

Use case

Cards leaked prior to a specific incident.

Goal

Analyze cards leaked before an incident that occurred in January 2025 by searching for cards detected up to December 31, 2024, for a specific BIN.

Query

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

#86 Teams: Anti-Fraud Team Context: Credit cards

Use case

Cards compromised in big leaks.

Goal

Identify compromised cards included in major, widely known breaches by searching for credit card numbers contained in large breach files.

Query

```
fileName="History.txt"
```

#87 Teams: Anti-Fraud Team Context: Credit cards

Use case

Cards with CVV available for fraud.

Goal

Detect cards with CVV information available—making them more vulnerable to fraud—by filtering for records where the CVV field is present for a specific BIN.

Query

```
cvv=* AND bin=123456
```

#88 Teams: Anti-Fraud Team Context: Credit cards

Use case

Executive credit cards found in leaks.

Goal

Locate executives’ credit cards exposed in leaks by filtering across multiple cardholder names to identify cards possibly tied to executives or key individuals within the organization.

Busca

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

#89 Teams: Blue Team, Anti-Fraud Team Context: Ads & Paid Search

Use case

Ads impersonating the brand but not redirecting to the official site.

Goal

Search for Meta-sponsored ads impersonating the brand that do not redirect to the company’s official website. Such cases can serve as phishing vectors.

Query

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

#91 Teams: Blue Team, Anti-Fraud Team Context: Ads & Paid Search

Use case

Common ad templates.

Goal

Identify ads using the same template (collation). This information can help uncover fraudster patterns and campaign replication strategies.

Query

```
collationId=12312437816347236
```

#90 Teams: Blue Team, Anti-Fraud Team Context: Ads & Paid Search

Use case

Profile IDs creating large volumes of fraudulent ads.

Goal

Investigate and gather evidence on profiles spreading large numbers of fraudulent ads. Often these profiles avoid using the company logo, making detection and removal more difficult.

Query

```
metaProfileId=12312437816347236
```

#92

Teams: Blue Team, Anti-Fraud Team

Context: Ads & Paid Search

Use case

Common profile names in fraud campaigns.

Goal

Investigate suspicious profiles with common or fake-sounding names that may be creating large volumes of fraudulent ads.

Query

```
metaProfileName="{{Profile Name}}"
```

#93

Teams: Blue Team, Anti-Fraud Team

Context: Ads & Paid Search

Use case

Brand color scheme in fraudulent ads.

Goal

Search for ads using the brand's color scheme. Even when fraudsters avoid logos, they often replicate the brand's visual identity through colors to attract victims.

Query

```
predominantColorHex=#FE3131
```

#94

Teams: Blue Team, Anti-Fraud Team

Context: Ads & Paid Search

Use case

Use of the brand name in ad descriptions.

Goal

Search for occurrences of the brand name or specific phrases frequently used by the brand, such as slogans, within ad descriptions.

Query

```
adDescription={{companyName}}
```

#95

Teams: Blue Team, Anti-Fraud Team

Context: URLs & Domínios

Use case

Pages using the company's favicon.

Goal

Search for pages that use the company's favicon, either by filename or by hash, to identify fraudulent domains visually mimicking the brand.

Query

```
resourceFilename="nficon2016.ico"

resourceHash=29dd20bc4b9b45bb7e0898e27af633320c9ae2b3e89d933f7aa6522ba238f171
```

★ Top Search #96 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domínios

Use case

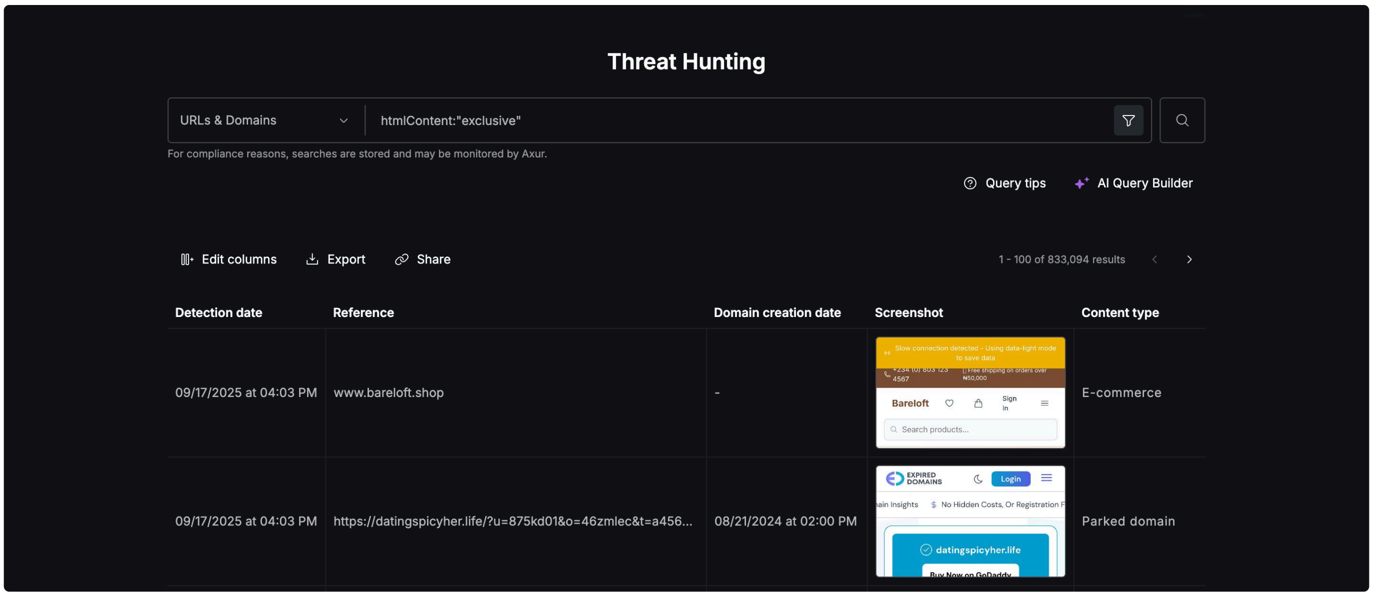
Text in HTML.

Goal

Search for text within the HTML source—for example, phrases commonly used by the brand on its official site, as well as unique identifiers such as tax IDs, phone numbers, or addresses.

Query

```
htmlContent:"exclusive"
```



Threat Hunting

URLs & Domains | htmlContent:"exclusive"

For compliance reasons, searches are stored and may be monitored by Axur.

1 - 100 of 833,094 results

Detection date	Reference	Domain creation date	Screenshot	Content type
09/17/2025 at 04:03 PM	www.bareloft.shop	-		E-commerce
09/17/2025 at 04:03 PM	https://datingspicyher.life/?u=875kd01&o=46zmlec&t=a456...	08/21/2024 at 02:00 PM		Parked domain

Slow connection detected - Using data-light mode to save data
Bareloft
Sign In
Search products...
EXPIRED DOMAINS
Login
No Hidden Costs, Or Registration F
datingspicyher.life
Buy Now on GoDaddy

#97 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domínios

Use case

Files containing the brand name.

Goal

Search for filenames such as company_logo.png to identify pages reusing the same artifacts as the official site.

Query

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

#98 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domínios

Use case

Font used in a phishing kit.

Goal

Search for a specific font file commonly used in a phishing kit to detect fraudulent pages.

Query

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

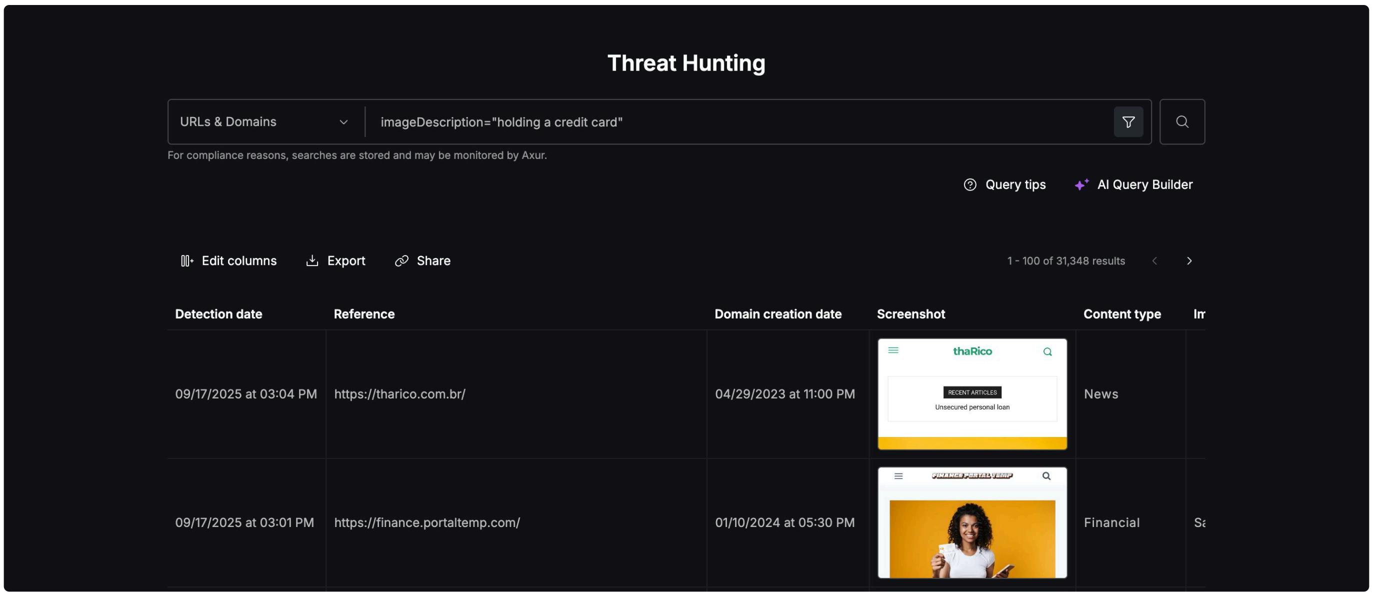
★ Top Search **99** Teams: Blue Team, Anti-Fraud Team Context: URLs & Domínios

Use case **Image descriptions from screenshots.**

Goal Search for screenshot image descriptions, using elements such as “holding a credit card.”

Busca

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



Threat Hunting

URLs & Domains | imageDescription="holding a credit card"

For compliance reasons, searches are stored and may be monitored by Axur.

Query tips · AI Query Builder

Edit columns · Export · Share · 1 - 100 of 31,348 results

Detection date	Reference	Domain creation date	Screenshot	Content type	Im
09/17/2025 at 03:04 PM	https://tharico.com.br/	04/29/2023 at 11:00 PM	thaRico RECENT ARTICLES Unsecured personal loan	News	
09/17/2025 at 03:01 PM	https://finance.portaltemp.com/	01/10/2024 at 05:30 PM		Financial	Sa

#100 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domínios

Use case **No open ports.**

Goal Search for recently created domains that do not yet have ports 80 or 443 open.

Query

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

#101 Teams: Blue Team, Anti-Fraud Team Context: URLs & Domínios

Use case **Terms in final redirect URLs.**

Goal Search for specific terms commonly found in phishing kits that appear only in the final redirect URLs, such as produto or checkout.

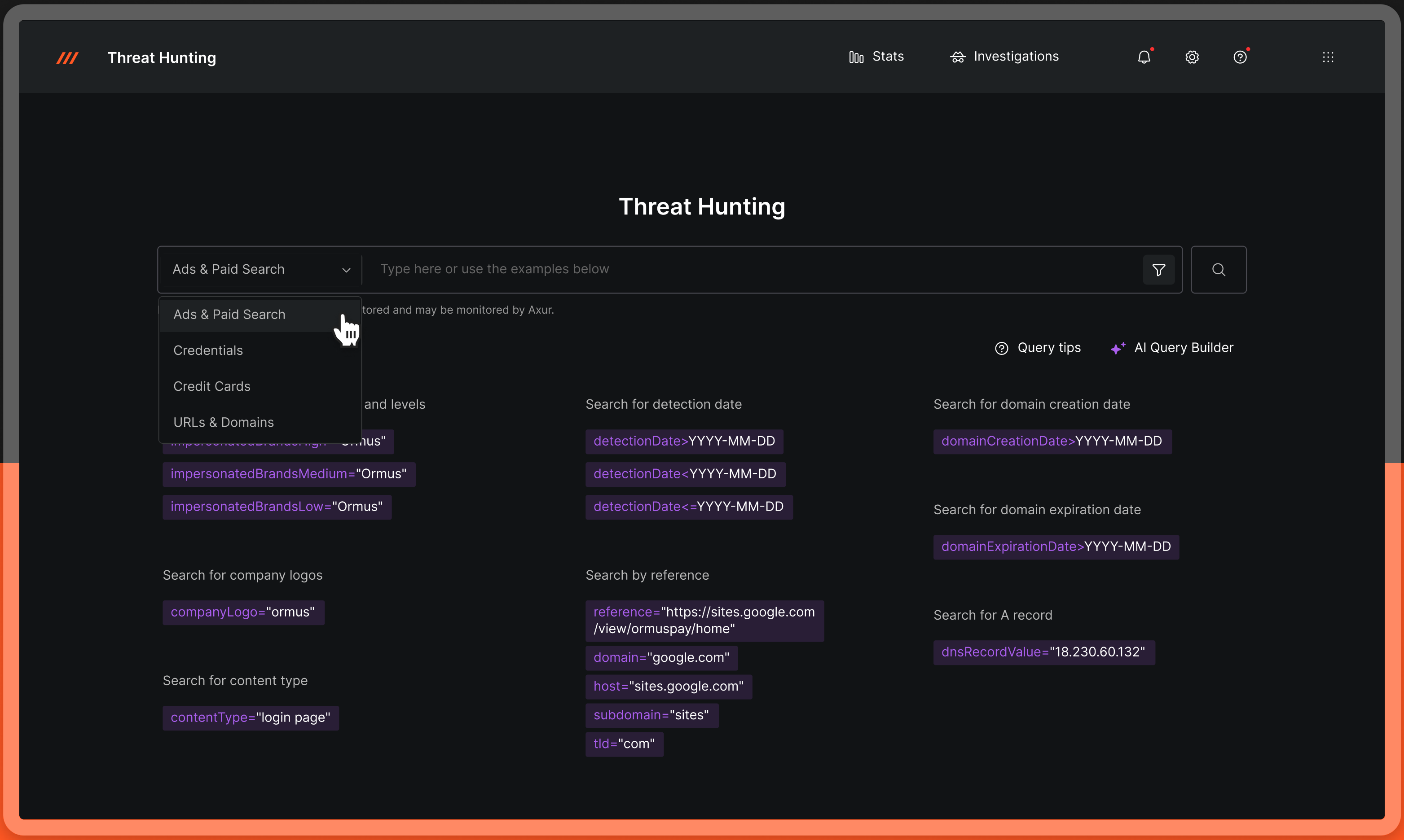
Query

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

Discover Threat Hunting

The 101 Threat Hunting use cases from Axur show that external threat detection is not a one-time task, but an ongoing practice to reduce risk across multiple areas of the organization.

Each use case highlights how credentials, digital assets, and exposed information can be exploited in different ways—and how anticipation changes the game in response. The key takeaway is clear: the more visibility you have into what circulates outside your systems, the stronger your ability to protect your business effectively.



Threat Hunting

Ads & Paid Search | Type here or use the examples below

Ads & Paid Search
Credentials
Credit Cards
URLs & Domains

…tored and may be monitored by Axur.

Query tips | AI Query Builder

…and levels

…impersonatedBrandsHigh="Ormus"

impersonatedBrandsMedium="Ormus"

impersonatedBrandsLow="Ormus"

Search for company logos

companyLogo="ormus"

Search for content type

contentType="login page"

Search for detection date

detectionDate>YYYY-MM-DD

detectionDate<YYYY-MM-DD

detectionDate<=YYYY-MM-DD

Search by reference

reference="https://sites.google.com/view/ormuspay/home"

domain="google.com"

host="sites.google.com"

subdomain="sites"

tld="com"

Search for domain creation date

domainCreationDate>YYYY-MM-DD

Search for domain expiration date

domainExpirationDate>YYYY-MM-DD

Search for A record

dnsRecordValue="18.230.60.132"

Gain access to one of the world's largest malicious data repositories.

GET A DEMO

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Gartner Peer Insights 4.9 ★★★★★

Discover all our solutions: **axur.com**

///AXUR