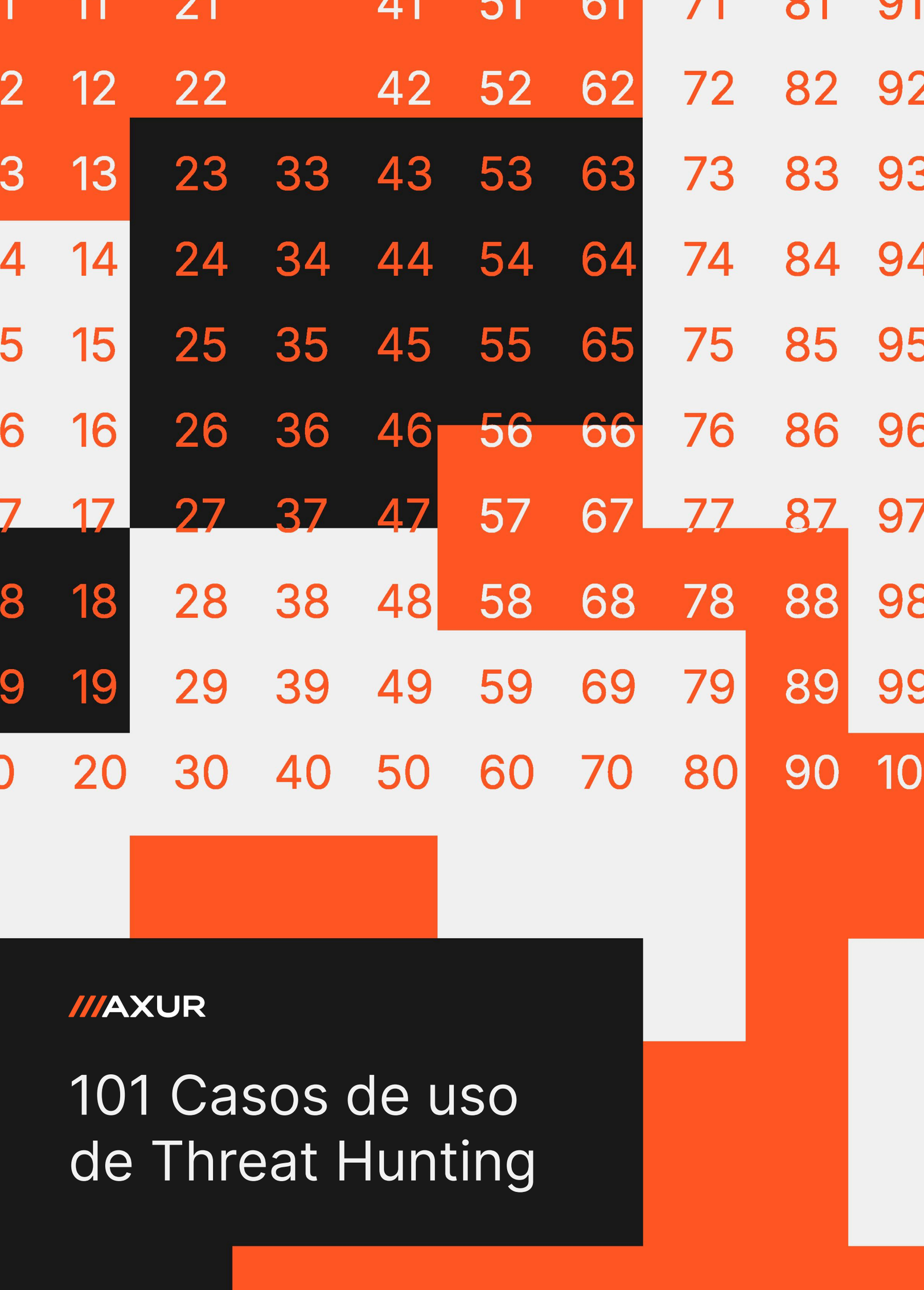

AXUR
101 Casos de uso
de Threat Hunting

Sumario

Casos de uso reales, resultados inmediatos

Threat Hunting es una herramienta avanzada de investigación dentro de la plataforma de Axur. Permite a los usuarios realizar búsquedas en una base de datos sumamente rica que abarca credenciales, tarjetas, anuncios, URLs y dominios.
Para ayudarte a obtener el máximo valor de la herramienta, hemos recopilado casos de uso reales que muestran cómo nuestros clientes y socios están aprovechando la solución.

Son 101 maneras de realizar búsquedas y obtener mejores resultados en tus investigaciones.

Busca amenazas e incidentes tanto dentro como fuera de tus activos monitoreados y aprovecha todo el potencial de la base de datos maliciosa más grande, respaldada por un modelo de IA que detecta amenazas de forma visual y contextual en cualquier idioma, enriqueciendo y priorizando cada señal.

- Casos de uso estratégicos
- Respuesta a amenazas e incidentes
- Investigación profunda para mitigar riesgos

Top Search **#01** Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso

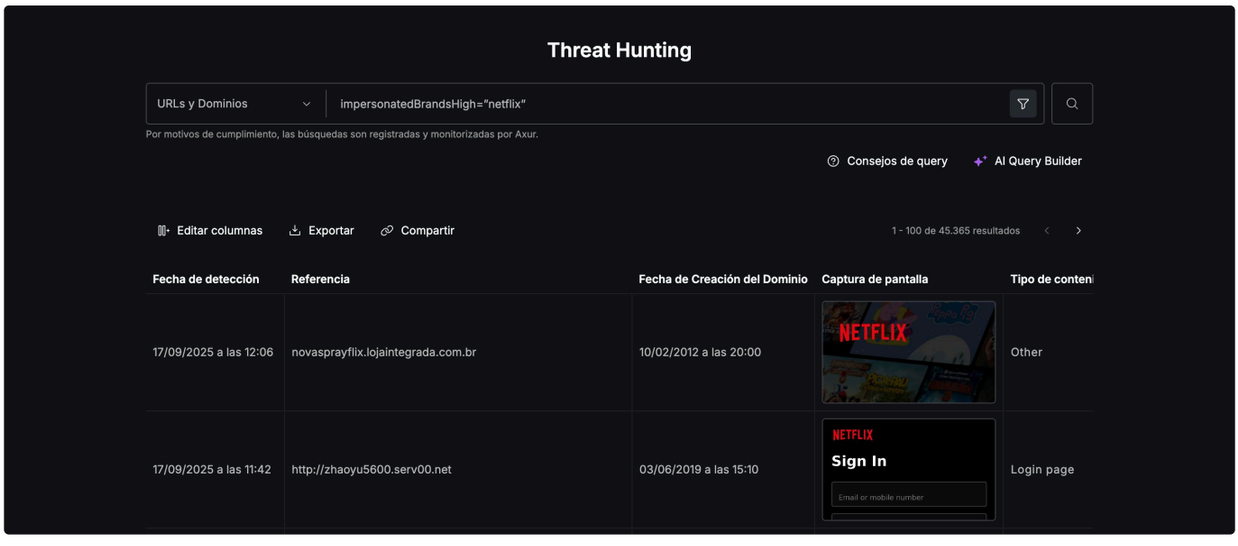
Identificación de campañas con un alto nivel de personificación visual y textual de la identidad de la empresa.

Objetivo

Identificar campañas con un alto nivel de personificación visual y textual, buscando dominios estrechamente asociados a la marca y páginas que imitan de forma evidente la identidad de la empresa.

Búsqueda

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



#02 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

Identificación de campañas estacionales (y de competidores) a través de páginas relacionadas con fechas conmemorativas.

Objetivo

Identificar campañas estacionales amplias en el sector, buscando páginas relacionadas con fechas conmemorativas. Como variación más específica, es posible incluir competidores en el filtro, por ejemplo: `impersonatedBrandsHigh="amazon"`.

Búsqueda

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

#03 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

URLs maliciosas recién registradas en el sector financiero (adaptable a otros sectores).

Objetivo

Identificar URLs maliciosas registradas recientemente en el sector financiero, con posibilidad de adaptar el mismo enfoque a otros sectores según la necesidad.

Búsqueda

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

#04 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso **Detección de TLDs populares en fraudes financieros y de comercio electrónico.**

Objetivo Identificar dominios con TLDs populares en fraudes financieros y de e-commerce, como .shop, detectando amenazas en sitios que simulan tiendas en línea.

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

#05 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso **Amenazas de phishing financiero con dominios de pago.**

Objetivo Identificar amenazas de phishing financiero que utilizan dominios con temática de pago, como el TLD .pay, simulando páginas de pago.

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

#06 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso **Dominios reservados para campañas futuras e inactivos.**

Objetivo Identificar dominios reservados como preparación para campañas futuras, buscando aquellos registrados en los últimos 90 días que estén inactivos, sin contenido o marcados como “parked”.

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

#07 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso **Dominios que devuelven error utilizados en ataques intermitentes (on/off).**

Objetivo Identificar dominios que devuelven error y pueden usarse en ataques que “encienden y apagan” páginas falsas en determinados horarios, buscando páginas clasificadas como “error page”.

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

#08 Equipos: Legal, Compliance — Contexto: URLs y Dominios

Caso de uso: **Dominios relacionados con actividades de apuestas que utilizan la marca de la empresa.**

Objetivo: Identificar dominios vinculados a actividades de apuestas que usan o asocian la marca de la empresa, buscando contenido clasificado como “gambling” y que incluya menciones a la marca en ese contexto.

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

#09 Equipos: Legal, Compliance — Contexto: URLs y Dominios

Caso de uso: **Dominios que aparentan ser fuentes de noticias para desinformación.**

Objetivo: Investigar dominios que aparentan ser portales de noticias, buscando contenido clasificado como “news” donde la empresa sea mencionada en imágenes o en el HTML. Estos sitios pueden imitar grandes medios de comunicación para difundir desinformación o manipular. Como variación, se puede buscar únicamente por el uso del logotipo de la empresa, por ejemplo: `companyLogo={{company}}`.

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

#10 Equipos: Blue Team, Anti-Fraud — Contexto: URLs y Dominios

Caso de uso: **Páginas financieras falsas que imitan bancos y fintechs.**

Objetivo: Detectar páginas financieras falsas que simulan instituciones legítimas, ya sea de una empresa específica o de todo el sector financiero. La búsqueda puede centrarse en contenido clasificado como “financial”, identificando páginas que imitan bancos, fintechs u operadores de tarjetas.

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

#11 Equipos: Blue Team, Anti-Fraud — Contexto: URLs y Dominios

Caso de uso: **Páginas falsas de inicio de sesión para capturar credenciales.**

Objetivo: Identificar páginas falsas de inicio de sesión creadas para capturar credenciales, buscando contenido clasificado como “login page”.

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

#12 Equipos: Legal, Compliance Contexto: URLs y Dominios

Caso de uso

Fraudes de e-commerce con productos inexistentes.

Objetivo

Identificar fraudes que utilizan páginas de e-commerce falsas con productos inexistentes o clonados, buscando contenido clasificado como “e-commerce” en páginas que mencionan a la empresa y que estén en dominios registrados en los últimos 90 días.

Búsqueda

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

#13 Equipos: Legal, Compliance Contexto: URLs y Dominios

Caso de uso

Páginas con contenido adulto asociadas a la marca de la empresa.

Objetivo

Identificar páginas con contenido adulto que vinculan la marca de la empresa, buscando sitios clasificados como “adult” que mencionen a la compañía.

Búsqueda

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

#14 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

Dominios y hosts que utilizan el nombre exacto de la marca.

Objetivo

Identificar dominios y hosts que emplean el nombre de la marca, verificando la presencia exacta de este en el dominio o en el host.

Búsqueda

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

#15 Equipos: Blue Team Contexto: URLs y Dominios

Caso de uso

Campañas de phishing operadas desde una misma región geográfica.

Objetivo

Mapear campañas de phishing originadas en una misma región geográfica, utilizando datos de geolocalización para identificar clusters de ataques asociados a la marca, alojados en ISPs específicos, como en Rusia.

Búsqueda

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

Top Search #16 — Equipos: Blue Team, Anti-Fraud — Contexto: URLs y Dominios

Caso de uso

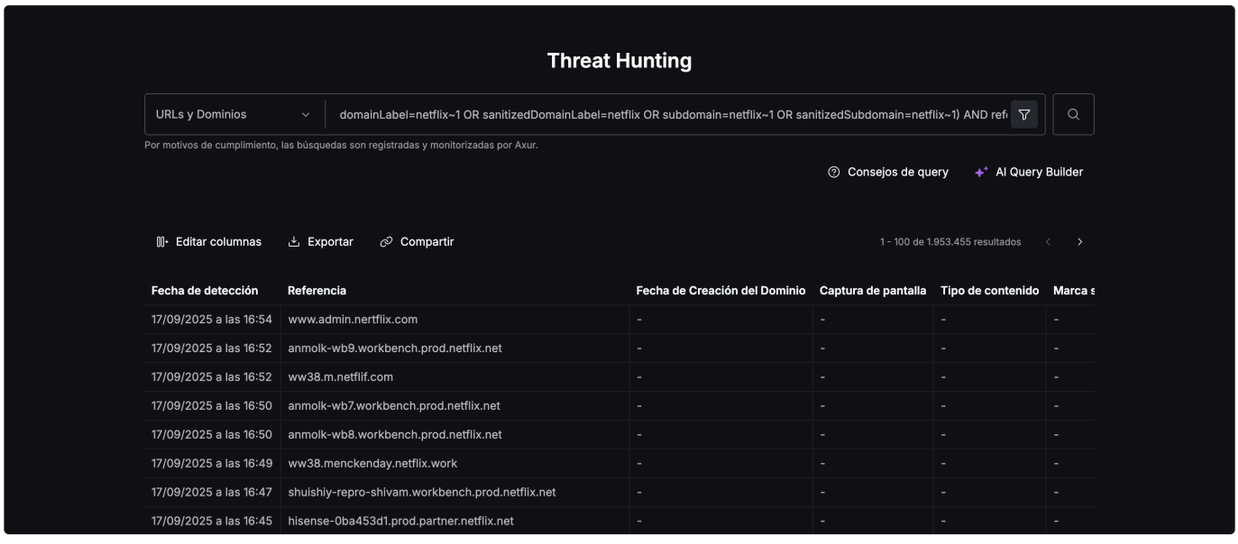
Dominios y hosts similares a la marca con variaciones y homógrafos.

Objetivo

Identificar dominios y hosts similares a la marca, buscando la presencia de la misma en el dominio con variaciones, incluyendo typos y homógrafos.

Búsqueda

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



#17 — Equipos: Blue Team — Contexto: URLs y Dominios

Caso de uso

Campañas de phishing operadas desde una misma región geográfica.

Objetivo

Mapear campañas de phishing originadas en una misma región geográfica, utilizando datos de geolocalización para identificar clusters de ataques asociados a páginas de inicio de sesión de Microsoft y Apple, alojadas en ISPs de Rusia.

Búsqueda

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

#18 — Equipos: Blue Team — Contexto: URLs y Dominios

Caso de uso

Campañas de phishing que utilizan el mismo ISP.

Objetivo

Investigar campañas de phishing que emplean el mismo ISP, identificando páginas falsas que comparten la misma infraestructura de alojamiento.

Búsqueda

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

Top Search #19 — Equipos: Blue Team, Anti-Fraud — Contexto: URLs y Dominios

Caso de uso

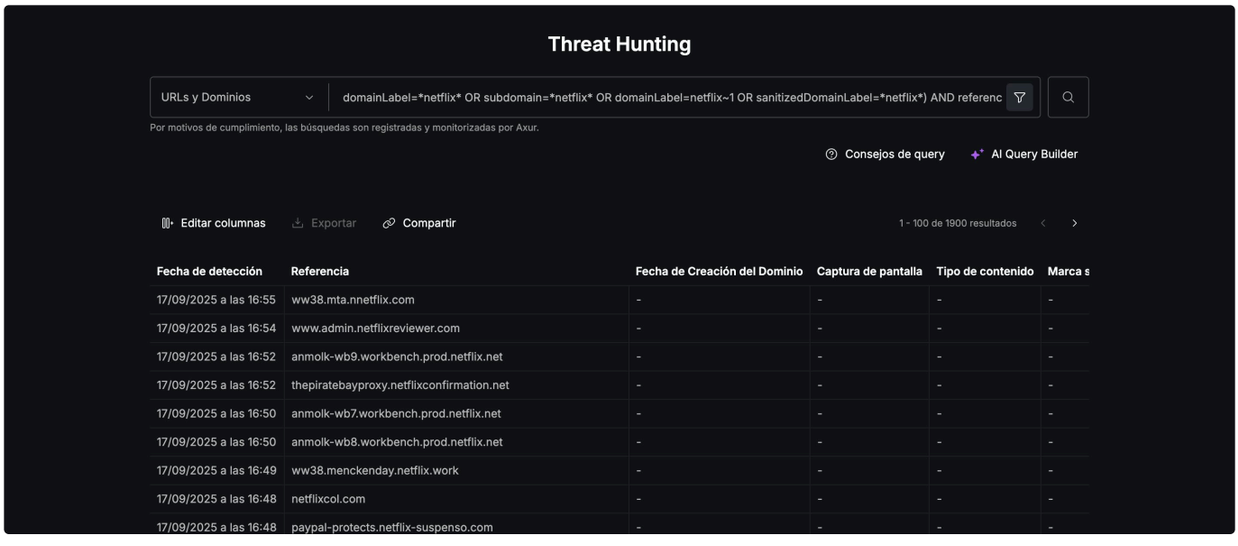
Búsqueda amplia de dominios similares con gran volumen de detecciones.

Objetivo

Identificar dominios y hosts similares a la marca, buscando la presencia de la misma en cualquier parte del dominio con variaciones, incluyendo typos y homógrafos. Dependiendo de la marca, esta búsqueda puede generar un volumen muy alto de detecciones.

Búsqueda

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



#20 — Equipos: Blue Team — Contexto: URLs y Dominios

Caso de uso

Páginas que solicitan datos de pago asociadas a la marca.

Objetivo

Analizar páginas que solicitan datos de pago vinculados a la marca, buscando aquellas con formularios de pago relacionados con la empresa o con el sector.

Búsqueda

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

#21 — Equipos: Blue Team — Contexto: URLs y Dominios

Caso de uso

URLs que utilizan las marcas Visa, Mastercard y la marca de la empresa.

Objetivo

Investigar URLs que utilizan las marcas Visa, Mastercard y la marca de la empresa, buscando páginas en las que Visa o Mastercard aparezcan mencionadas junto con la marca de la compañía.

Búsqueda

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

#22 Equipos: Blue Team Contexto: URLs y Dominios

Caso de uso

Validación de URL sospechosa en múltiples bases especializadas.

Objetivo

Validar si una URL sospechosa figura en múltiples bases especializadas de phishing, verificando si el dominio ya está listado como malicioso y obteniendo una confirmación con mayor cobertura.

Búsqueda

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

#23 Equipos: Blue Team, Anti-Fraud Contexto: Anuncios y Búsqueda Pagada

Caso de uso

Páginas maliciosas promovidas mediante campañas pagadas en Facebook Ads.

Objetivo

Investigar páginas maliciosas difundidas a través de campañas pagadas en Facebook Ads, identificando URLs falsas patrocinadas que utilizan la marca y consolidando una lista de esas URLs anunciadas.

Búsqueda

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

#24 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

Campañas vinculadas al mismo perfil tras la detección de fraude.

Objetivo

Buscar campañas asociadas a un mismo perfil después de la detección de fraude a través de anuncios en Facebook Ads, mapeando el historial de campañas fraudulentas relacionadas con ese mismo operador.

Búsqueda

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

#25 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

Fraudes promovidos por el mismo enlace de anunciante tras una campaña engañosa.

Objetivo

Rastrear fraudes promovidos por el mismo enlace de anunciante después de una campaña engañosa, identificando otras campañas vinculadas a la misma URL y consolidando una lista de campañas fraudulentas ejecutadas por el mismo perfil.

Búsqueda

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

Top Search #26 Equipos: Blue Team, Anti-Fraud, Legal, Compliance Contexto: URLs y Dominios

Caso de uso

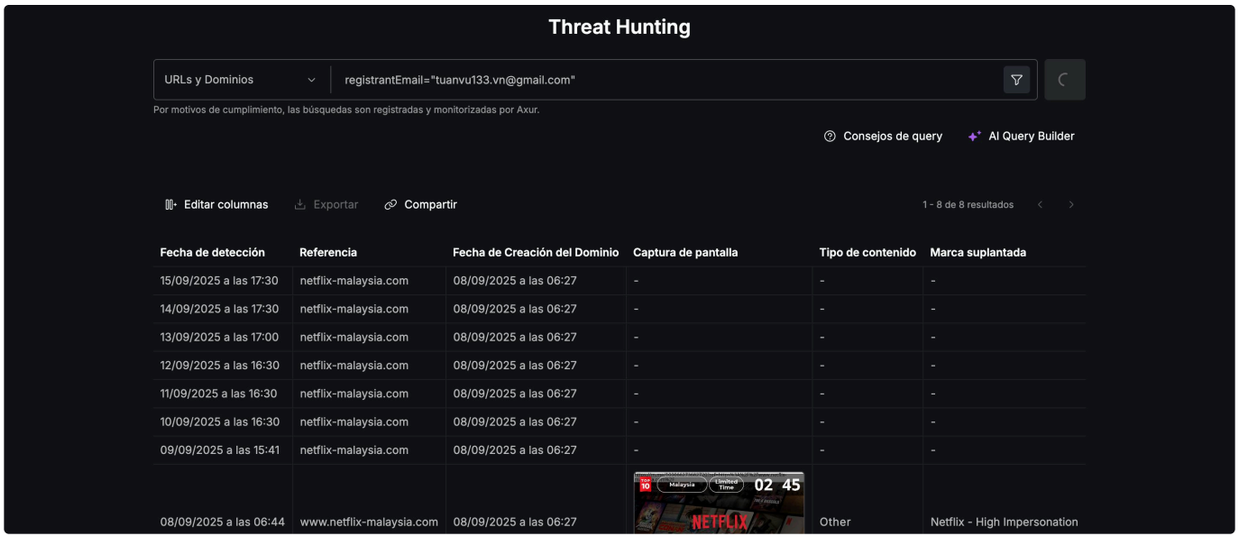
Páginas maliciosas asociadas al mismo registrante o correo electrónico.

Objetivo

Investigar páginas maliciosas vinculadas al mismo registrante o correo de registro, identificando fraudes de campañas que reutilizan información de WHOIS y detectando posibles páginas fraudulentas creadas por el mismo registrante.

Búsqueda

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



#27 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

Campañas recientes alojadas por proveedores como Cloudflare.

Objetivo

Investigar campañas recientes alojadas en proveedores como Cloudflare, correlacionando amenazas que utilizan la misma infraestructura de hospedaje e identificando dominios maliciosos recientes asociados al mismo ISP.

Búsqueda

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

#28 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

Campañas que comparten la misma infraestructura de DNS.

Objetivo

Investigar campañas que utilizan la misma infraestructura de DNS, identificando dominios vinculados a campañas anteriores que comparten los mismos name servers y detectando posibles fraudes relacionados con la reutilización de DNS.

Búsqueda

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

#29 Equipos: Blue Team Contexto: URLs y Dominios

Caso de uso

Páginas potencialmente utilizadas para capturar credenciales corporativas.

Objetivo

Identificar páginas potencialmente diseñadas para capturar credenciales corporativas, buscando sitios falsos de plataformas como Google y Microsoft en dominios que mencionan la marca del cliente. El objetivo es detectar campañas de phishing dirigidas a empleados con el fin de robar credenciales de acceso corporativo.

Búsqueda

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

#30 Equipos: Blue Team, Anti-Fraud Team Contexto: URLs y Dominios

Caso de uso

Dominios posiblemente utilizados para spear phishing sin página web activa.

Objetivo

Identificar dominios posiblemente empleados en ataques de spear phishing, buscando aquellos que suplantan la marca de la empresa, poseen registros MX configurados para el envío de correos electrónicos, pero no tienen página web activa.

Búsqueda

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

#31 Equipos: Legal, Compliance Contexto: URLs y Dominios

Caso de uso

Vinculación de la marca con contenidos inapropiados como juegos de azar.

Objetivo

Detectar la vinculación de la marca con contenidos inapropiados, como juegos de azar, buscando páginas clasificadas como “gambling” que muestren el logotipo de la empresa.

Búsqueda

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

#32 Equipos: Anti-Fraud Team Contexto: URLs y Dominios

Caso de uso

Páginas potencialmente utilizadas para fraudes en otros países.

Objetivo

Identificar páginas potencialmente usadas para fraudes en otros países, buscando aquellas que suplantan la marca en diferentes idiomas y en regiones donde la empresa no tiene presencia.

Búsqueda

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

#33 Equipos: Blue Team Contexto: URLs y Dominios

Caso de uso	**Contenido malicioso alojado en subdominios propios inactivos.**
Objetivo	Detectar contenido malicioso alojado en subdominios de la empresa que deberían estar inactivos, investigando casos de subdomain hijacking. La investigación debe generar una lista de subdominios configurados con registros CNAME que apuntan a proveedores de alojamiento externos, permitiendo evaluar cuáles están vulnerables o siendo utilizados de manera indebida.
Búsqueda	`domain=company.com AND (dnsRecordType=CNAME AND dnsRecordValue=(*.github.io OR *.herokuapp.com OR *.s3.amazonaws.com OR *.cloudfront.net OR *.wordpress.com))`

#34 Equipos: Anti-Fraud Team Contexto: URLs y Dominios

Caso de uso	**Detección de dominios con uso exclusivo de IPv6 y registro AAAA para identificar configuraciones intencionales de evasión.**
Objetivo	Identificar dominios que utilizan exclusivamente IPv6 y mencionan a la empresa, buscando dominios sospechosos con solo registro AAAA. El uso exclusivo de IPv6 puede indicar una configuración intencional para evadir la detección, ya que algunas herramientas y firewalls todavía ofrecen menor cobertura para IPv6.
Búsqueda	`dnsRecordType="AAAA" AND NOT dnsRecordType=A AND companiesMentioned=google`

#35 Equipos: Anti-Fraud Team Contexto: URLs y Dominios

Caso de uso	**Páginas con uso indebido del logotipo de la marca sin mención textual en el dominio.**
Objetivo	Identificar páginas que emplean el logotipo de la marca sin mencionar el nombre de la empresa en la URL, detectando el uso indebido de elementos visuales sin relación textual en el dominio.
Búsqueda	`companyLogo={{company}} AND NOT reference=*{{company}}*`

#36 Equipos: Anti-Fraud Team Contexto: URLs y Dominios

Caso de uso	**Dominios recientes (60 días) que utilizan la marca en sus páginas.**
Objetivo	Identificar páginas que hacen uso de la marca, buscando dominios registrados en los últimos 60 días que contengan páginas vinculadas a la empresa.
Búsqueda	`domainCreationDate>=2025-07-01 AND companiesMentioned={{company}}`

Top Search #37 — Equipos: Blue Team, Anti-Fraud — Contexto: URLs y Dominios

Caso de uso

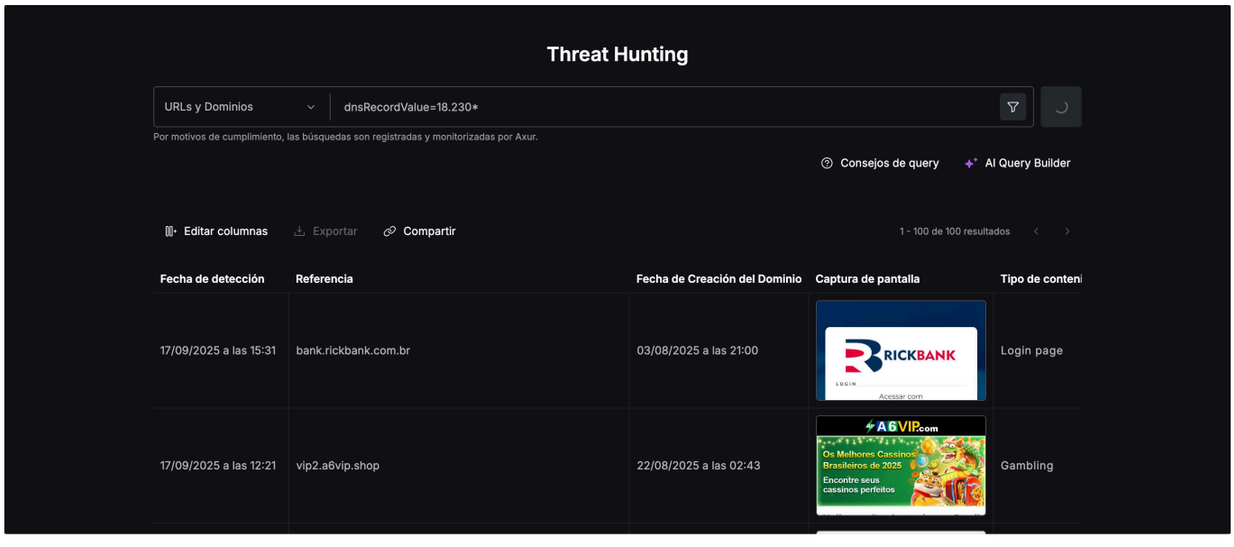
Campañas que comparten el mismo bloque de IPs.

Objetivo

Investigar campañas que comparten el mismo bloque de IPs (sextetos u octetos), buscando, a partir de una página falsa identificada, otras páginas asociadas a la misma infraestructura.

Búsqueda

```
dnsRecordValue=18.230*
```



#38 — Equipos: Anti-Fraud — Contexto: URLs y Dominios

Caso de uso

Uso indebido de nombres de ejecutivos para la promoción no autorizada de productos o servicios.

Objetivo

Verificar el uso indebido de nombres de ejecutivos fuera de contextos periodísticos, identificando páginas que explotan esos nombres para promover la venta de productos o servicios sin autorización.

Búsqueda

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

#39 — Equipos: Anti-Fraud — Contexto: URLs y Dominios

Caso de uso

Investigación de sitios falsos que imitan el soporte técnico de la empresa para capturar datos personales.

Objetivo

Investigar casos en los que clientes afirman haber introducido datos personales en sitios falsos que imitaban el soporte técnico de la empresa, buscando páginas que mencionen la marca, soliciten contraseñas y simulen atención al usuario, incluyendo palabras como “help” o “customer” en la URL.

Búsqueda

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

#40 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Páginas falsas de competidores (especialmente de inicio de sesión) para anticipar ataques.**
Objetivo	Identificar ataques de páginas falsas contra competidores para anticipar amenazas, buscando páginas con un alto nivel de suplantación de esas marcas, registradas en los últimos 90 días. Como variación más específica, es posible filtrar únicamente páginas cuyo contentType="login page", priorizando aquellas que imitan áreas de autenticación de los competidores.
Búsqueda	`(impersonatedBrandsHigh="competitor A" OR impersonatedBrandsHigh="competitor B") AND domainCreationDate>2025-06-30`

#41 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Identificación de campañas con uso parcial de elementos de la marca y suplantación media.**
Objetivo	Identificar campañas con uso parcial de elementos de la marca, detectando fraudes con nivel medio de suplantación en páginas que presentan elementos moderadamente relacionados con la marca. Este enfoque puede generar un mayor volumen de casos, pero resulta útil para identificar situaciones fuera del patrón habitual.
Búsqueda	`impersonatedBrandsMedium="{{company}}"`

#42 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Detección de campañas iniciales o sutiles con bajo nivel de suplantación de la marca.**
Objetivo	Detectar campañas iniciales o sutiles que utilizan la marca, identificando casos de suplantación de bajo nivel. Este enfoque puede generar un volumen mayor de resultados, pero es útil para descubrir amenazas en etapas tempranas o situaciones atípicas.
Búsqueda	`impersonatedBrandsLow="{{company}}"`

#43 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Identificación de páginas que mencionan a la empresa en sitios clasificados como “financial”.**
Objetivo	Identificar páginas que mencionan a la empresa en su contenido textual o visual, buscando referencias a la marca en sitios clasificados como “financial”.
Búsqueda	`companiesMentioned="{{company}}" AND contentType="financial"`

#44 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Verificación del uso del logotipo de la empresa en dominios potencialmente maliciosos clasificados como “financial”.**
Objetivo	Verificar el uso del logotipo de la empresa en dominios potencialmente maliciosos, buscando la presencia de elementos visuales de la marca en sitios clasificados como “financial”.
Búsqueda	`companyLogo="{{company}}" AND contentType="financial"`

#45 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Rastreo de simulaciones visuales de aplicaciones que mencionan el nombre de la marca de la empresa.**
Objetivo	Rastrear simulaciones visuales de aplicaciones, identificando páginas con apariencia de apps que mencionan el nombre de la marca de la empresa.
Búsqueda	`imageDescription=({{company}} AND "mobile app")`

#46 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Detección de dominios con enlaces a Telegram que mencionan la marca de la empresa.**
Objetivo	Detectar dominios que contienen enlaces a Telegram y mencionan la marca, identificando páginas que hacen referencia a la empresa y contienen enlaces HTML externos hacia grupos o perfiles en Telegram.
Búsqueda	`htmlLinks=t.me AND companiesMentioned="{{company}}"`

#47 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Identificación de páginas que redirigen a números o grupos de WhatsApp para fraudes directos.**
Objetivo	Identificar páginas que redirigen a números o grupos de WhatsApp, detectando fraudes realizados mediante contactos directos en la plataforma. La investigación genera una lista de páginas que fomentan la comunicación directa con estafadores vía WhatsApp.
Búsqueda	`impersonatedBrandsHigh="{{company}}" AND htmlLinks=wa.me`

#48 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Investigación de fraudes organizados en servidores o grupos de Discord con enlaces HTML.**
Objetivo	Investigar fraudes organizados en servidores o grupos de Discord, identificando páginas que contienen enlaces HTML que hacen referencia a grupos en la plataforma. El objetivo es detectar campañas o comunidades ilegítimas que operan a través de Discord.
Búsqueda	`impersonatedBrandsHigh="{{company}}" AND htmlLinks=discord.gg`

#49 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Identificación de fraudes que dirigen a las víctimas hacia números de WhatsApp y rastreo de campañas asociadas.**
Objetivo	Identificar fraudes que redirigen a las víctimas hacia números de WhatsApp y, a partir de la detección de un número fraudulento, rastrear otras páginas vinculadas a la misma campaña criminal.
Búsqueda	`htmlLinks=*11922331092*`

#50 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Dominios maliciosos activos que personifican la marca, especialmente los recientes y aún operativos.**
Objetivo	Identificar dominios maliciosos activos que personifican la marca, especialmente aquellos creados recientemente y que todavía se encuentran operativos (no suspendidos).
Búsqueda	`impersonatedBrandsHigh="{{company}}" AND domainCreationDate>=2025-06-01` `AND NOT domainStatus="suspended"`

#51 Equipos: Anti-Fraud Contexto: URLs y Dominios

Caso de uso	**Páginas con acortadores de URL que enmascaran ataques mencionando la marca.**
Objetivo	Identificar y detectar páginas que utilizan acortadores de URL (como Bit.ly, TinyURL, etc.) para enmascarar las URLs finales, mencionando una marca y empleando estos redireccionadores populares como puente para ataques, generando una lista de las URLs implicadas.
Búsqueda	`htmlLinks=("bit.ly" OR "tinyurl.com" OR "t.co" OR "cutt.ly" OR "is.gd")` `AND companiesMentioned="{{company}}"`

#52 Equipos:: Anti-Fraud Contexto: URLs y Dominios

Caso de uso **Intentos de phishing con dominios similares a la empresa utilizando el operador "fuzzy".**

Objetivo Identificar posibles intentos de phishing buscando dominios similares a la empresa (con el operador "fuzzy"), para listar dominios semejantes a "{{company}}" que puedan estar siendo usados para engañar a los usuarios.

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

#53 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Tácticas de recolección de credenciales del sector y credenciales filtradas de sitios web específicos.**

Objetivo Mapear tácticas comunes de recolección de credenciales en el sector e identificar credenciales filtradas de acceso a un sitio web específico, utilizando solo el dominio o la URL completa.

Búsqueda `accessUrl={{company.com}}`

#54 Equipos: Red & Blue Teams, Legal Contexto: Credenciales

Caso de uso **Riesgo de seguridad de proveedores a través de la exposición de credenciales de empleados.**

Objetivo Evaluar el riesgo de seguridad al contratar a un proveedor, buscando exposiciones de las credenciales de sus empleados.

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

#55 Equipos: Red & Blue Teams Contexto: Credenciales

Caso de uso **Exposición previa de un empleado en fuentes de alto riesgo y en la deep/dark web.**

Objetivo Identificar la exposición previa de un empleado en fuentes de alto riesgo, investigando filtraciones relacionadas con un usuario específico y determinando si la fuente corresponde a la deep/dark web.

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

#56 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Credenciales filtradas con URL de acceso comprobable.**

Objetivo Verificar si una credencial filtrada tiene una URL de acceso disponible, buscando credenciales expuestas de la empresa que estén asociadas a una URL de acceso y que puedan ser probadas de forma inmediata en esa dirección.

Búsqueda `user="user@company.com" AND accessUrl=*`

#57 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Credenciales filtradas en un archivo específico.**

Objetivo Explorar archivos con grandes volúmenes de credenciales en venta en foros y, a partir de esta búsqueda, evaluar qué otras credenciales provienen de un archivo específico para comprender su contenido, el perfil de las víctimas y las posibles conexiones.

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

#58 Equipos: Blue Team, Legal Contexto: Credenciales

Caso de uso **Análisis de riesgos de socios estratégicos en filtraciones externas.**

Objetivo Investigar la exposición de socios estratégicos en filtraciones externas, evaluando el impacto indirecto de fugas estructuradas sobre estos socios para mapear el riesgo por asociación con terceros.

Búsqueda `fileName="leaked_suppliers.txt" AND *vendor*`

#59 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Exposición de credenciales corporativas a través de correo electrónico profesional.**

Objetivo Verificar si una credencial corporativa fue expuesta a través del correo electrónico profesional, buscando todas las credenciales filtradas que usen la dirección completa de un individuo.

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

#60 Equipos: Anti-Fraud, Blue Team — Contexto: Credenciales

Caso de uso	**Presencia de números de teléfono en filtraciones con credenciales asociadas.**
Objetivo	Verificar la presencia del número de teléfono de un cliente en filtraciones, buscando teléfonos con identificación de nombre de usuario y comprobando si existen credenciales asociadas; esto es muy útil en procesos de investigación y fraude.
Búsqueda	`user="+5511987654321" AND userType="PHONE"`

#61 Equipos: Blue Team — Contexto: Credenciales

Caso de uso	**Exposición completa de datos personales mediante múltiples identificadores.**
Objetivo	Investigar la exposición de múltiples datos relativos a la misma persona combinando correos, teléfonos, nombres de usuario y números de identificación en la búsqueda, para obtener una visión integral de la exposición de un individuo mediante varios identificadores.
Búsqueda	`user=("user123" OR "12345678900" OR "+5511987654321" OR "user@company.com")`

#62 Equipos: Blue Team — Contexto: Credenciales

Caso de uso	**Filtración de credenciales en grupos conocidos de Telegram.**
Objetivo	Investigar la filtración de credenciales en grupos notorios de Telegram, buscando credenciales expuestas publicadas, por ejemplo, en el grupo STARLINK.
Búsqueda	`messageChatName=STARLINK*`

#63 Equipos: Blue Team — Contexto: Credenciales

Caso de uso	**Contraseñas en texto plano relacionadas con el dominio corporativo.**
Objetivo	Identificar contraseñas en texto claro vinculadas al dominio corporativo de la empresa o de terceros, listando credenciales de la empresa cuyos passwords están almacenados en texto abierto.
Búsqueda	`emailDomain=company.com AND passwordType=PLAIN`

#64 Equipos: Blue Team Contexto: Credenciales

Caso de uso	**Credenciales en formato hash asociadas a la empresa.**
Objetivo	Encontrar credenciales almacenadas como hashes, listando aquellas asociadas a la empresa.
Búsqueda	`emailDomain=company.com AND passwordType=(MD5 OR SHA1 OR MYSQL323)`

#65 Equipos: Blue Team Contexto: Credenciales

Caso de uso	**Exposición de credenciales de empleados en filtraciones de proveedores.**
Objetivo	Verificar la exposición de credenciales de empleados en filtraciones de proveedores, buscando credenciales de la empresa vinculadas a direcciones de acceso a herramientas del proveedor.
Búsqueda	`accessUrl=partner.com AND emailDomain=company.com`

#66 Equipos: Blue Team Contexto: Credenciales

Caso de uso	**Credenciales corporativas en grandes filtraciones sectoriales.**
Objetivo	Identificar credenciales corporativas en una gran filtración del sector, buscando credenciales de la empresa asociadas a un archivo específico de dicho incidente.
Búsqueda	`fileName="leak.txt" AND emailDomain=company.com`

#67 Equipos: Blue Team Contexto: Credenciales

Caso de uso	**Análisis de reutilización de contraseñas en casos de fraude.**
Objetivo	Analizar el caso de un cliente que reutilizó contraseñas y fue víctima de fraude, buscando credenciales reutilizadas en diferentes plataformas con distintos nombres de usuario.
Búsqueda	`user=(customer@example.com OR "Username" OR 12345678910)`

#68 Equipos:: Blue Team Contexto: Credenciales

Caso de uso **Intentos múltiples de inicio de sesión con credenciales expuestas y contraseñas débiles.**

Objetivo Investigar intentos múltiples de inicio de sesión reportados por un cliente, buscando credenciales expuestas con contraseñas consideradas débiles.

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

#69 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Presencia de la empresa en filtraciones masivas de foros clandestinos.**

Objetivo Detectar la presencia de la empresa o de sus clientes en una filtración masiva identificada, buscando ocurrencias dentro de un archivo específico citado en foros clandestinos.

Búsqueda
```
fileName="Collection1.txt" AND emailDomain="company.com"
```

#70 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Contraseñas débiles de la empresa en filtraciones ampliamente divulgadas.**

Objetivo Verificar contraseñas débiles en filtraciones ampliamente conocidas, explorando un archivo específico en busca de contraseñas vulnerables asociadas a la empresa.

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

#71 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Credenciales de empleado filtradas por reutilización de un nombre de usuario externo.**

Objetivo Identificar si un empleado tuvo credenciales de acceso expuestas, buscando por un nombre de usuario utilizado externamente y detectando el uso previo del mismo en filtraciones.

Búsqueda
```
user="user123"
```

#72 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Presencia de identificadores de empleados en filtraciones.**

Objetivo Confirmar la presencia de identificadores de empleados en filtraciones, buscando números de identificación corporativa que puedan considerarse datos sensibles.

Búsqueda `"123456789000012"`

#73 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Nombres completos expuestos en filtraciones públicas.**

Objetivo Investigar el uso indebido de nombres completos en filtraciones públicas, buscando exposiciones con nombre textual, lo que puede ayudar a encontrar información relevante sobre individuos específicos.

Búsqueda `"John Doe"`

#74 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Intentos bloqueados por autenticación multifactor.**

Objetivo Detectar intentos de acceso detenidos por autenticación multifactor, buscando repeticiones de la misma contraseña en diferentes filtraciones, lo cual resulta útil para encontrar otros nombres de usuario del mismo individuo cuando la contraseña es muy específica.

Búsqueda `password="password123"`

#75 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Usuarios con acceso privilegiado a APIs internas.**

Objetivo Identificar la exposición de usuarios específicos con acceso a APIs internas, buscando credenciales vinculadas a sistemas internos o gestores, y listando accesos críticos con alto nivel de privilegio (usuarios estándar).

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

#76 Equipos: Blue Team Contexto: Credenciales

Caso de uso **Cuentas administrativas en sistemas heredados.**

Objetivo Verificar la filtración de cuentas administrativas en sistemas heredados, identificando “admin”, “root” o “webmaster” asociadas a IPs internos o localhost (usuarios estándar).

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

#77 Equipos: Anti-Fraud Contexto: Credenciales

Caso de uso **Credenciales comprometidas de aplicaciones móviles.**

Objetivo Identificar credenciales vinculadas al uso de aplicaciones, evaluando credenciales comprometidas que acceden a una aplicación específica y listando aquellas expuestas asociadas a dicho app mediante su Google Play ID.

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

#78 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Tarjetas de crédito filtradas de otras instituciones.**

Objetivo Mapear fuentes de filtración de tarjetas recurrentes en el sector, buscando BINs de tarjetas de otras instituciones financieras que hayan sido expuestas.

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

#79 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Tarjetas de la empresa en la deep & dark web.**

Objetivo Identificar tarjetas de la empresa circulando en la Deep Web, buscando aquellas con origen en la Deep/Dark Web que posiblemente estén en comercialización por actores maliciosos.

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

#80 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Tarjetas filtradas en grupos de Telegram.**

Objetivo Investigar la filtración de tarjetas en un grupo específico de Telegram, buscando tarjetas publicadas en un grupo reconocido de la plataforma.

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

#81 Equipos: Anti-Fraud Team Contexto: Tarjetas de Crédito

Caso de uso **Análisis de reembolso por cargos indebidos.**

Objetivo Analizar la solicitud de reembolso de un cliente que alega un cargo no autorizado, verificando si su tarjeta fue filtrada recientemente y utilizada en la transacción fraudulenta.

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

#82 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Compras no autorizadas en múltiples tarjetas.**

Objetivo Investigar compras no autorizadas realizadas por el mismo individuo en diferentes tarjetas, identificando múltiples tarjetas vinculadas al mismo titular.

Búsqueda `holder="John Doe"`

#83 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Datos ingresados en un sitio fraudulento.**

Objetivo Analizar el caso de un cliente engañado que introdujo datos en un sitio falso, investigando la exposición de tarjetas de crédito a partir de números parciales disponibles.

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

#84 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Tarjetas con fecha de expiración futura aún activas.**

Objetivo Evaluar el riesgo asociado a tarjetas cuya fecha de expiración es posterior a 2025 y que podrían seguir utilizándose de forma fraudulenta.

Búsqueda `expirationYear>=25 AND bin=123456`

#85 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Tarjetas filtradas antes de un incidente específico.**

Objetivo Analizar tarjetas filtradas con anterioridad a un incidente ocurrido en enero de 2025, buscando registros detectados hasta el 31 de diciembre de 2024 para un BIN determinado.

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

#86 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Tarjetas en grandes filtraciones conocidas.**

Objetivo Identificar tarjetas comprometidas que aparecen en grandes filtraciones ampliamente conocidas, examinando archivos de brechas masivas para localizar números de tarjetas afectados.

Búsqueda `fileName="History.txt"`

#87 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Tarjetas con CVV disponible para fraude.**

Objetivo Detectar tarjetas que incluyen CVV en los registros, más vulnerables al uso fraudulento, filtrando aquellas entradas que contienen el campo CVV para un BIN específico.

Búsqueda `cvv=* AND bin=123456`

#88 Equipos: Anti-Fraud Contexto: Tarjetas de Crédito

Caso de uso **Tarjetas de ejecutivos en filtraciones.**

Objetivo Localizar tarjetas de ejecutivos presentes en filtraciones, filtrando por múltiples nombres de titulares, con el fin de identificar tarjetas posiblemente vinculadas a ejecutivos o personas clave de la organización.

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

#89 Equipos: Blue Team, Anti-Fraud Contexto: Anuncios y Búsqueda Pagada

Caso de uso **Anuncios que suplantan la marca pero no redirigen al sitio oficial.**

Objetivo Buscar anuncios patrocinados en Meta que suplanten a una marca, pero que no redirijan al sitio oficial de la compañía. Estos casos pueden ser vectores de propagación de campañas de phishing.

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

#90 Equipos: Blue Team, Anti-Fraud Contexto: Anuncios y Búsqueda Pagada

Caso de uso **IDs de perfiles que generan múltiples anuncios fraudulentos.**

Objetivo Investigar y recopilar evidencias de que un perfil está difundiendo grandes cantidades de fraudes. Con frecuencia, los perfiles no utilizan el logotipo de la marca, lo que dificulta la identificación y eliminación.

Búsqueda
```
metaProfileId=12312437816347236
```

#91 Equipos: Blue Team, Anti-Fraud Contexto: Anuncios y Búsqueda Pagada

Caso de uso **Plantillas de anuncios recurrentes.**

Objetivo Identificar anuncios que utilizan la misma plantilla (collation). Esta información puede ser útil para reconocer patrones de los estafadores.

Búsqueda
```
collationId=12312437816347236
```

#92 Equipos: Blue Team, Anti-Fraud Contexto: Anuncios y Búsqueda Pagada

Caso de uso **Nombres de perfiles comunes en fraudes.**

Objetivo Investigar perfiles con nombres sospechosos que puedan estar generando numerosas actividades fraudulentas.

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

#93 Equipos: Blue Team, Anti-Fraud Contexto: Anuncios y Búsqueda Pagada

Caso de uso **Esquema de colores de la identidad visual de la marca.**

Objetivo Buscar esquemas de colores que identifiquen la identidad visual de una marca. En muchos anuncios, los estafadores no utilizan logotipos, pero sí reproducen la paleta de colores para atraer a las víctimas.

Búsqueda
```
predominantColorHex=#FE3131
```

#94 Equipos: Blue Team, Anti-Fraud Contexto: Anuncios y Búsqueda Pagada

Caso de uso **Uso del nombre de la marca en la descripción del anuncio.**

Objetivo Buscar el nombre de la marca o expresiones específicas frecuentemente utilizadas por ella, como eslóganes, en las descripciones de los anuncios.

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

#95 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso **Página con el favicon de la compañía.**

Objetivo Buscar páginas que utilizan el favicon de la compañía, ya sea mediante el nombre del archivo o a través de su hash.

Búsqueda
```
resourceFilename="nficon2016.ico"

resourceHash=29dd20bc4b9b45bb7e0898e27af633320c9ae2b3e89d933f7aa6522ba238f171
```

Top Search #96 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

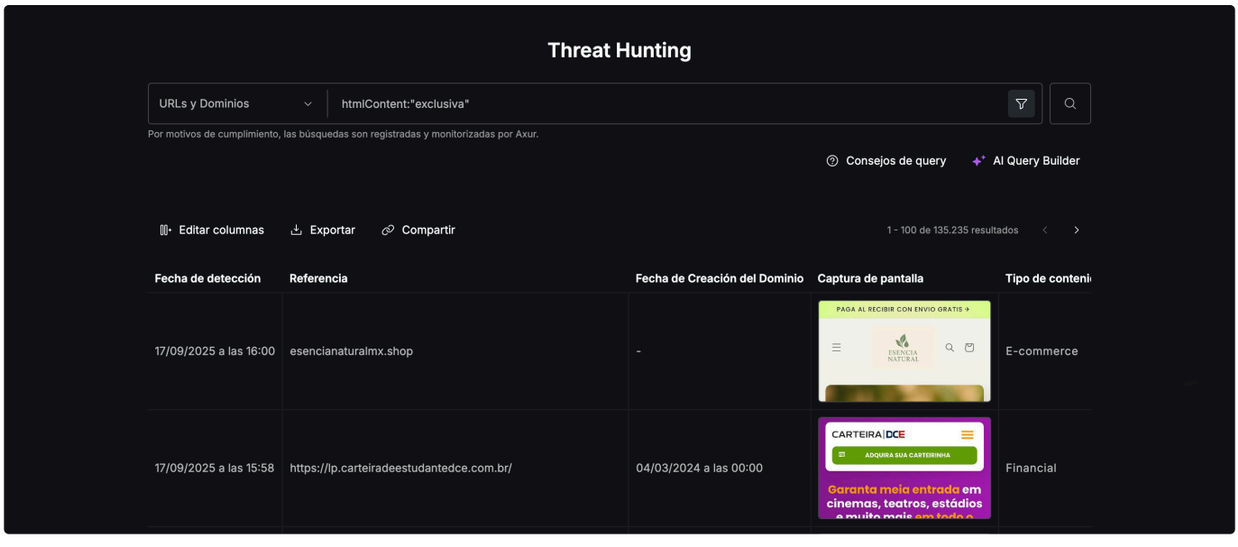
Texto en el HTML.

Objetivo

Buscar texto dentro del HTML, como frases utilizadas por la marca en su sitio oficial, así como identificadores únicos como números de teléfono o direcciones.

Búsqueda

```
htmlContent:"exclusiva"
```



#97 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

Archivos con el nombre de la marca.

Objetivo

Buscar nombres de archivos como company_logo.png para identificar páginas que reutilizan los mismos artefactos del sitio original.

Búsqueda

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

#98 Equipos: Blue Team, Anti-Fraud Contexto: URLs y Dominios

Caso de uso

Fuente utilizada en un kit de phishing.

Objetivo

Buscar una fuente específica empleada en un kit de phishing.

Búsqueda

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

Top Search 99 | Equipos: Blue Team, Anti-Fraud | Contexto: URLs y Dominios

Caso de uso

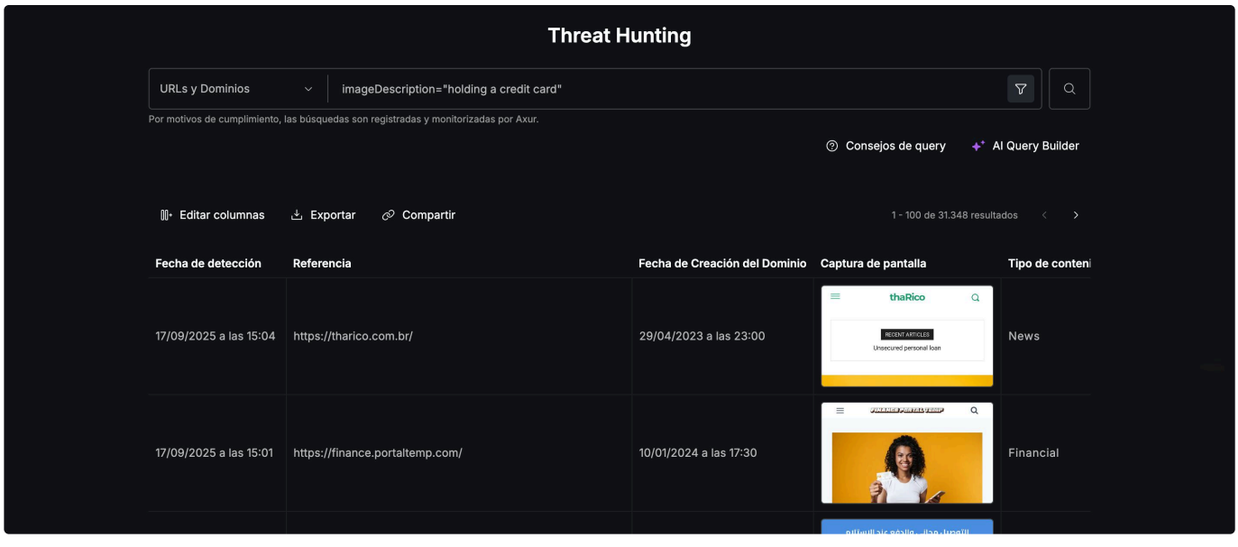
Descripciones de imágenes en capturas de pantalla.

Objetivo

Buscar descripciones de imágenes en capturas de pantalla, utilizando elementos como “mano sosteniendo una tarjeta de crédito”.

Busca

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



#100 | Equipos: Blue Team, Anti-Fraud | Contexto: URLs y Dominios

Caso de uso

Dominios sin puertos abiertos.

Objetivo

Buscar dominios creados recientemente que aún no tengan abiertos los puertos 80 y 443.

Búsqueda

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

#101 | Equipos: Blue Team, Anti-Fraud | Contexto: URLs y Dominios

Caso de uso

Términos en URLs finales de redireccionamiento.

Objetivo

Buscar términos específicos comunes en kits de phishing que solo aparecen en las URLs finales tras el redireccionamiento.

Búsqueda

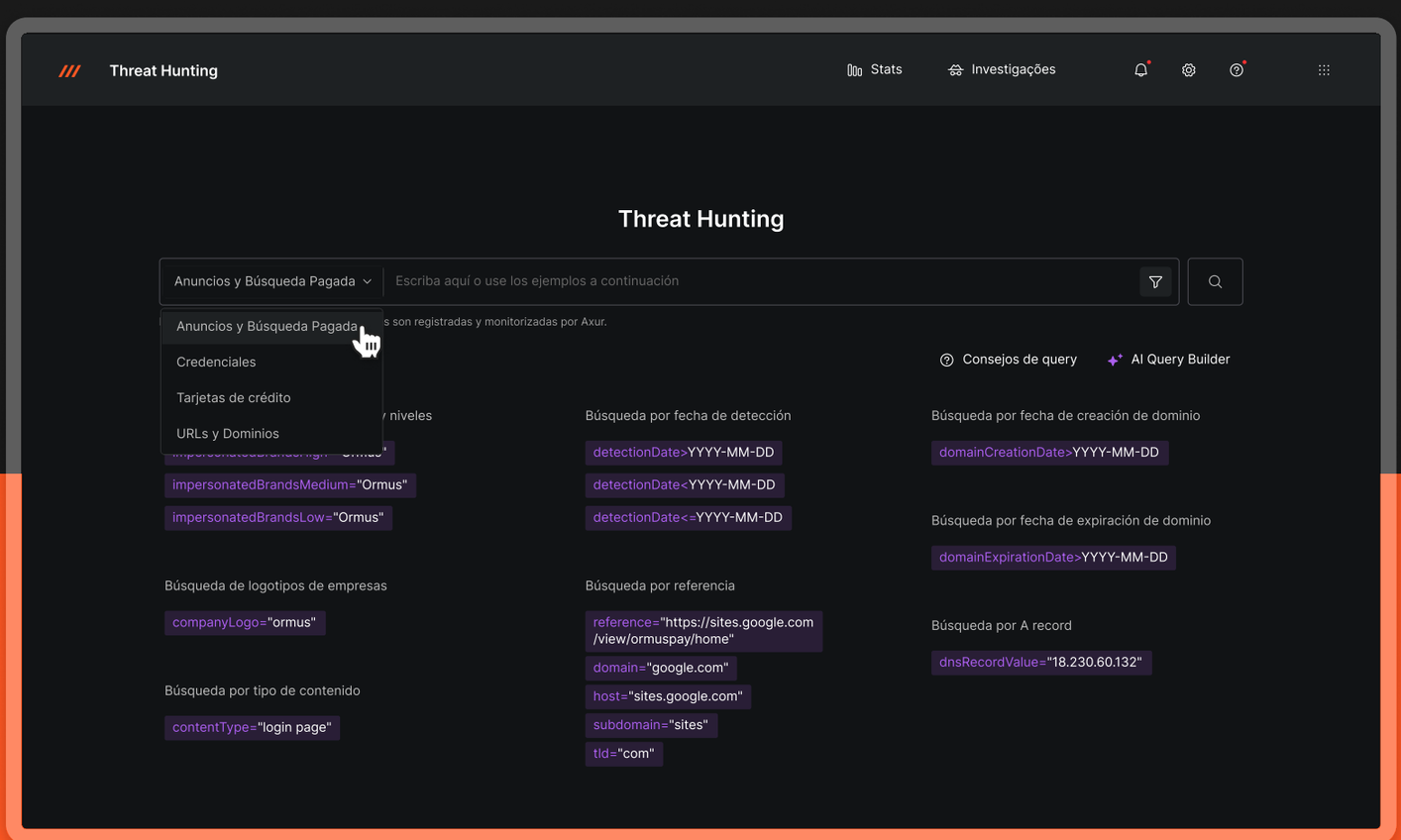
```
impersonatedBrandsHigh={{company}} AND (redirectedTo=product OR redirectedTo=checkout)
```

Prueba el Threat Hunting

Los 101 casos de uso de Threat Hunting de Axur demuestran que la detección de amenazas externas no es un ejercicio puntual, sino una práctica continua para reducir riesgos que se extiende a diversas áreas de la organización.

Cada caso evidencia cómo credenciales, activos digitales e información expuesta pueden ser explotados de diferentes maneras, y cómo la anticipación marca la diferencia en la respuesta.

La lección es clara: cuanto mayor sea la visibilidad sobre lo que circula fuera de sus sistemas, mayor será la capacidad de proteger eficazmente el negocio.



Obtenga acceso a una de las bases de datos de amenazas más grandes del mundo.

AGENDE UNA DEMO

ISO/IEC 27001 Information Security Management CERTIFIED

Gartner Peer Insights 4.9

Conozca todas nuestras soluciones: **axur.com**

AXUR