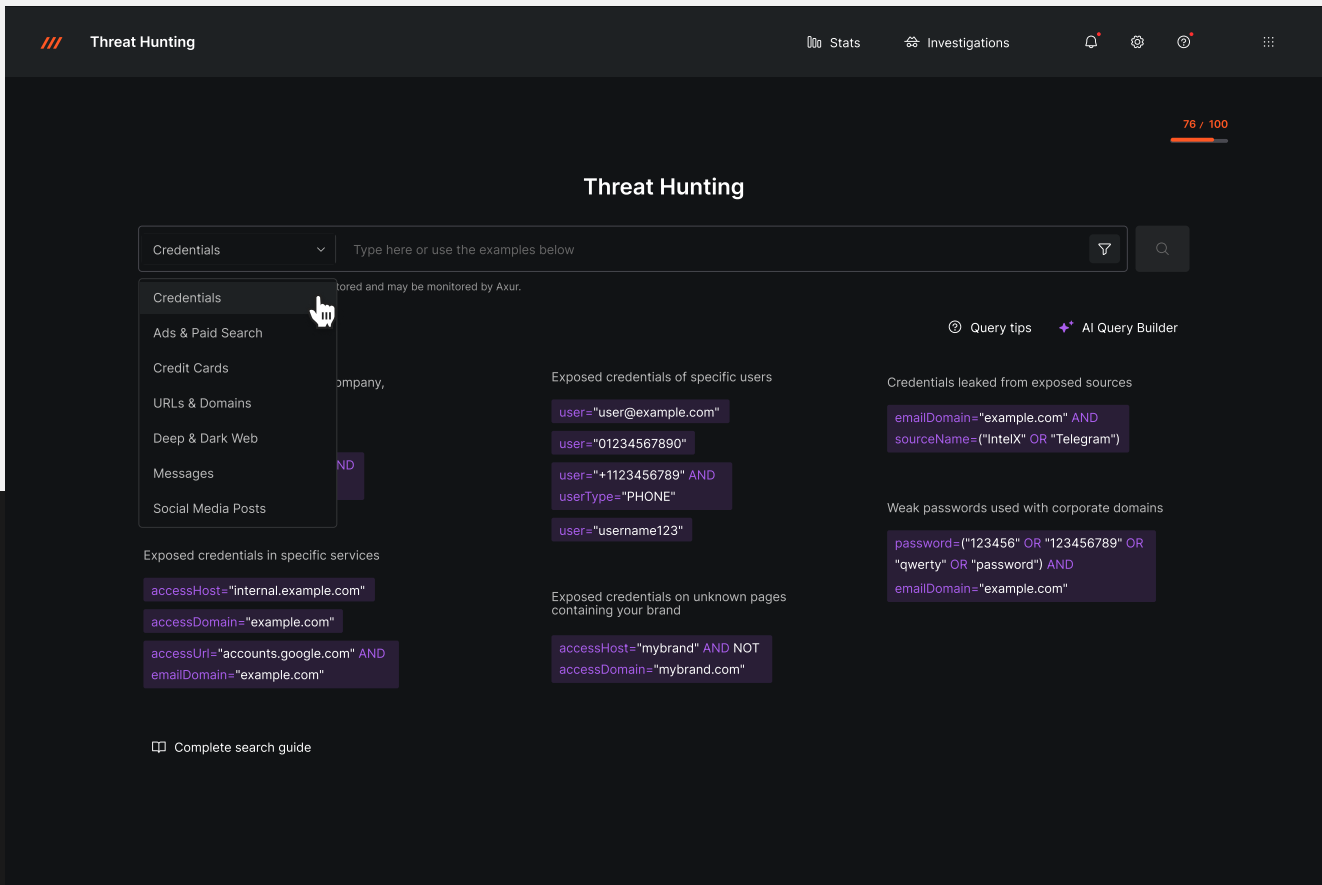


Enhance your investigations with Threat Hunting powered by one of the world's largest threat databases

As cyberattacks become more sophisticated, a proactive approach is essential. Threat Hunting dives deeper into relevant incidents, helping to reduce risks and accelerate your response to attacks.



Fictional data for demonstration purposes.

Threat Hunting lets you explore Axur's extensive database, conducting detailed searches for credentials, cards, leaked files, URLs, and domains.



Proactive hunting to Investigate and stop threats early.



Trend research to track attacks in your industry or competitors.



Third-Party investigations to assess vendor and partner security.

Discover how **Threat Hunting** can improve your security strategy

Credentials

Threat Hunting leverages a base of over 17 billion unique credentials exposed in data breaches and malware logs, helping you assess risks tied to vendors or customers, support audits, and prevent unauthorized access from leaked passwords.

Credit cards

Search for leaked credit card information to identify potential fraud risks early. This approach helps online businesses assess exposed payment data, flag suspicious transactions, and strengthen protective measures against financial threats.

URLs & Domains

Threat Hunting uncovers phishing sites and malicious domains, even without explicit brand mentions. This allows you to detect targeted phishing campaigns, monitor threat actor activities, and proactively protect against emerging online threats.

Introducing the **AI Query Builder:**

Leverage AI to create queries quickly and efficiently.

Supports:



ElasticSearch/
OpenSearch



Natural language
conversion to queries

AI Query Builder **BETA**

Hello, I'm the AI Query Builder! Tell me what you need, and I'll generate queries for you

Generating queries for

Generate

Don't know where to start?
Try it with one of the examples:

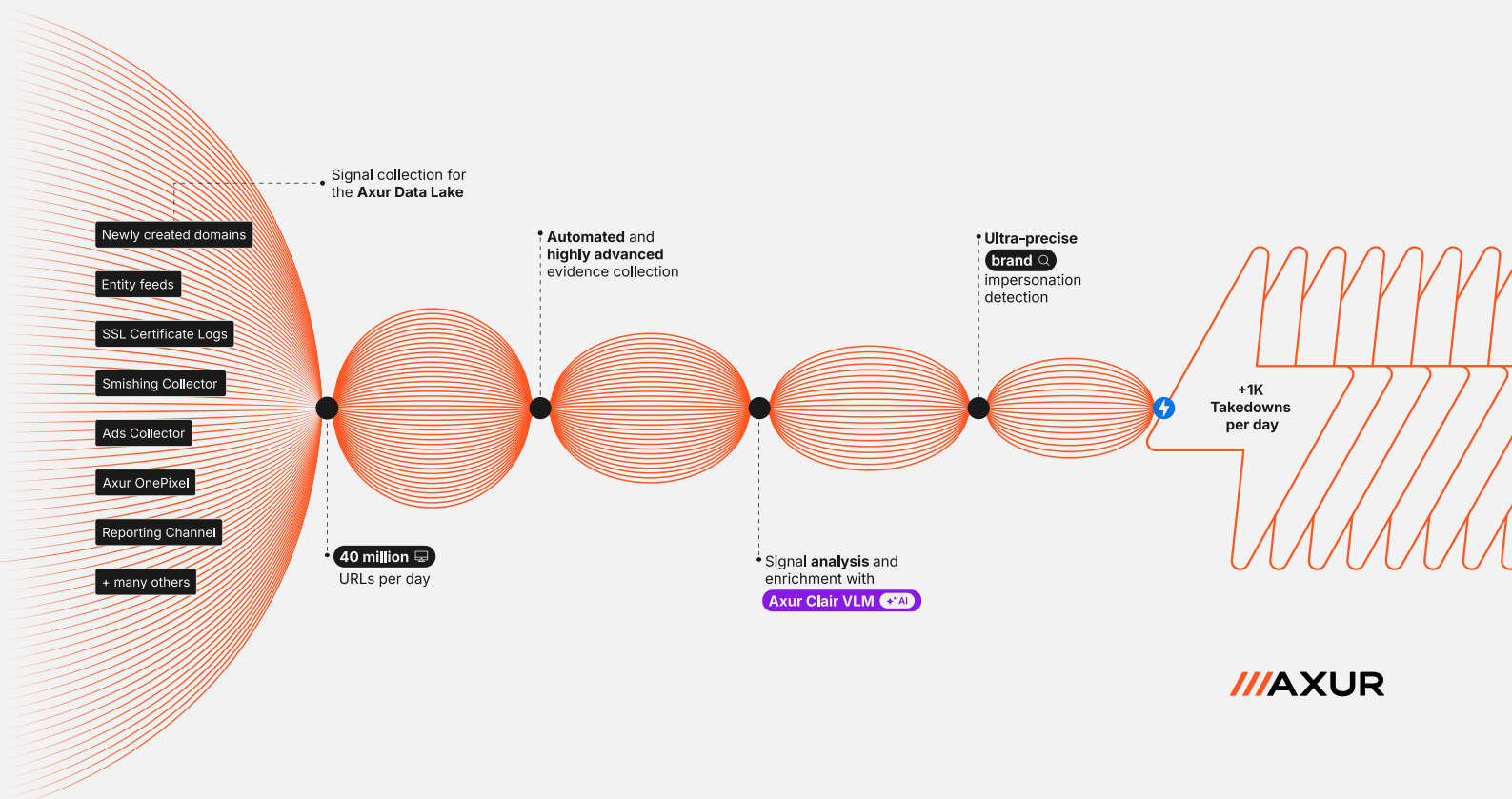
Phishing Scams Are Getting Smarter. And Harder to Catch

The screenshot displays the Axur Threat Hunting dashboard. At the top, there are navigation tabs for 'Stats' and 'Investigations', along with notification and settings icons. The main heading is 'Threat Hunting'. Below this, a search bar contains the query 'impersonatedBrandsHigh="Ormus"'. A note states: 'For compliance reasons, searches are stored and may be monitored by Axur.' Below the search bar, there are options for 'Query tips' and 'AI Query Builder'. The main content area shows a table with columns: 'Detection Date', 'Reference', 'Content type', and 'Screenshot'. The table contains three rows of data.

Detection Date	Reference	Content type	Screenshot
18/06/24 at 09:25	n/a	E-commerce	
18/06/24 at 09:25	healing-ormus.com	Financial	
18/06/24 at 09:25	ormus-holzspielzeug.de	Financial	


A fundamentally new approach to Brand Protection

We add 40 million new websites to our data lake daily. And use our GenAI models to inspect and enrich each signal.



AI-Enriched Signals

Our AI analyzes and enriches signals across multiple attributes, identifying:

Impersonated brands 

Companies mentioned and logos 

Content type and image descriptions 

Credentials requests 

Passwords and payment requests 

Typosquatting Detection









Uncover Hidden Threats

Overcome the keyword-based limitations by identifying deceptive domain variations designed to mislead users. Axur's Threat Hunting spots typosquatting and other domain manipulation tactics, ensuring comprehensive detection of threats that traditional methods might miss. This advanced detection keeps you protected from sophisticated tactics used to bypass common detection systems.


No Language Barriers



Detect phishing sites in any language, ensuring complete global protection.

Detect, Evaluate and Take Down Phishing Scams **Faster than Ever**

-  Completely automated takedown 24x7
-  Notification in <4min
-  98,9% success
-  9h median takedown time
-  15-day stay down guarantee
-  Web Safe Reporting
-  Follow up the whole process
-  We charge only for successful takedowns

 +1k takedowns per day

 1 notification sent, 1 reply

 facebook.com 

Received on 08/19/2024 at 11:03 PM

 Instagram.com 

First notification sent on 08/19/2024 at 10:58 PM

Threat moved to treatment

08/19/2024 at 10:58 PM

 Takedown requested automatically

08/19/2024 at 10:58 PM



Automation

Takedown, Instagram Logo, FSP

[Check automation](#)

Threat detected

08/19/2024 at 10:23 PM

Ready to See for Yourself?

REQUEST A DEMO

Discover all our solutions at axur.com

Gartner
Peer Insights..  4.9
 ★★★★★



AXUR