

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.

The screenshot shows the Axur Threat Hunting interface. At the top, there are navigation tabs for 'Stats' and 'Investigations', along with notification, settings, and help icons. A search bar at the top right shows 'Search requisitions 13 / 100'. The main heading is 'Threat Hunting'. Below it, a search filter is set to 'emailDomain=ormus.com,ormuspay.com'. A dropdown menu is open, showing 'Credentials', 'Credit Cards', and 'URLs & Domains'. The search results are displayed in a table with the following columns: Date, Email, Password, Password Type, and Source.

		Password	Password Type	Source
01/15/ 24 at 08:30	alice.williams@ormus.com	T*****	PLAIN	IntelX
01/15/ 24 at 08:30	bob.smith@ormus.com	g*****	PLAIN	IntelX
02/22/24 at 03:45	carol.jones@ormuspay.com	↑*****	SHA1	Mega
03/09/24 at 11:56	david.brown@ormus.com	h*****	PLAIN	Breachforums
04/17/24 at 06:15	emma.davis@ormuspay.com	M*****	PLAIN	Telegram
05/03/24 at 12:00	frank.miller@ormuspay.com	s*****	PLAIN	Telegram
06/26/24 at 04:30	hank.moore@ormus.com	D*****	PLAIN	IntelX
07/14/24 at 09:00	mia.hall@ormuspay.com	L*****	SHA1	Mega
08/30/24 at 07:15	ana.lopes@ormus.com	↑*****	PLAIN	Breachforums

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 42 billion 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.

Infected Machines

Track compromised devices using malware metadata through Threat Hunting. This helps you identify potential internal threats, contain infections early, and prevent them from spreading across your network.

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 **URLs & Domains**

I want suggestions for searching for...

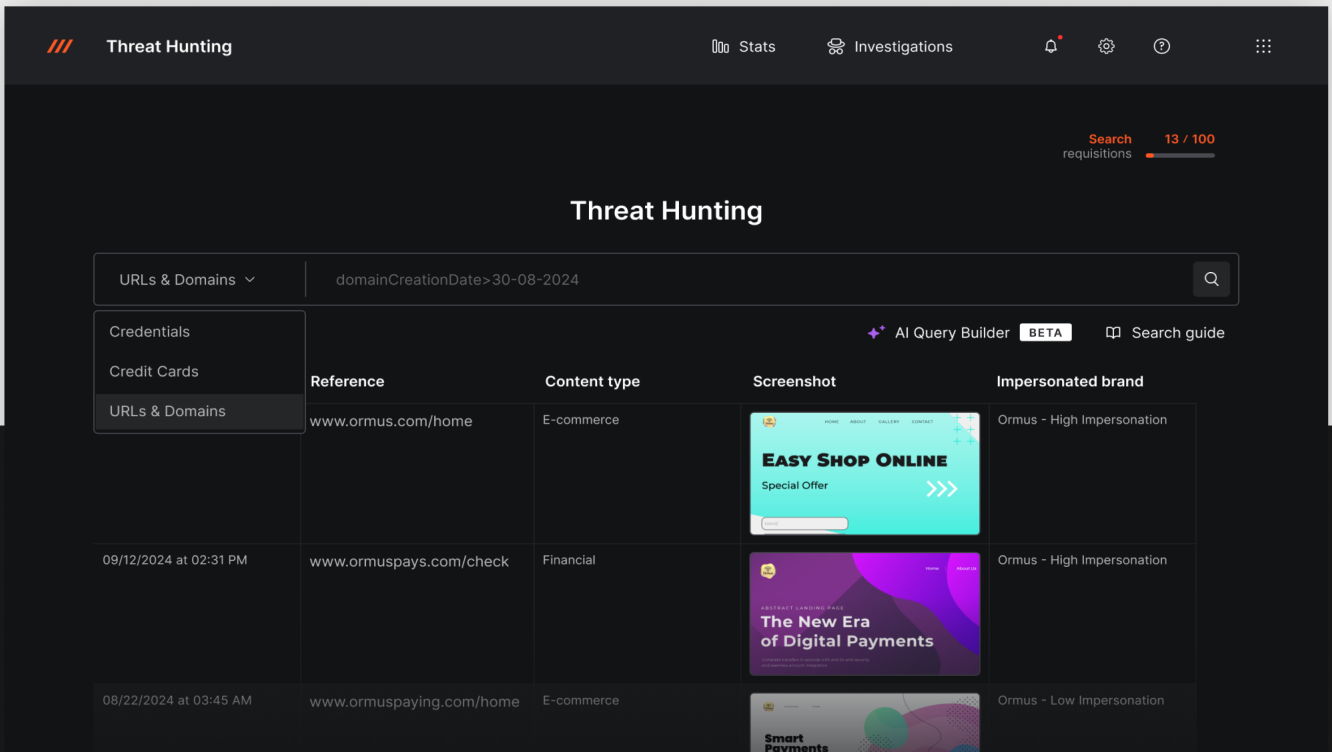
+ Generate

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

URLs of the domain ormus.com in the last 3 months

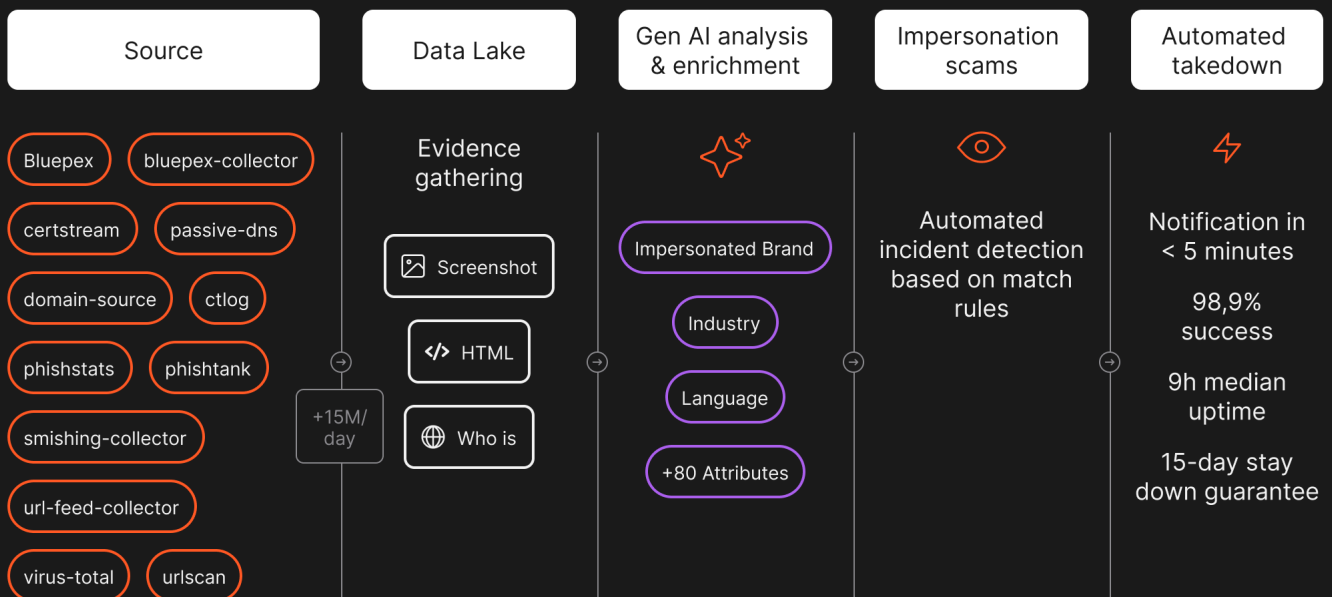
Domains displaying the logo of company Ormus

Phishing Scams Are Getting Smarter. And Harder to Catch




A fundamentally new approach to Brand Protection


We add 15 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 <5min
-  98,9% success
-  9h median uptime
-  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



CleanDNS
Trusted Reporter 

AXUR