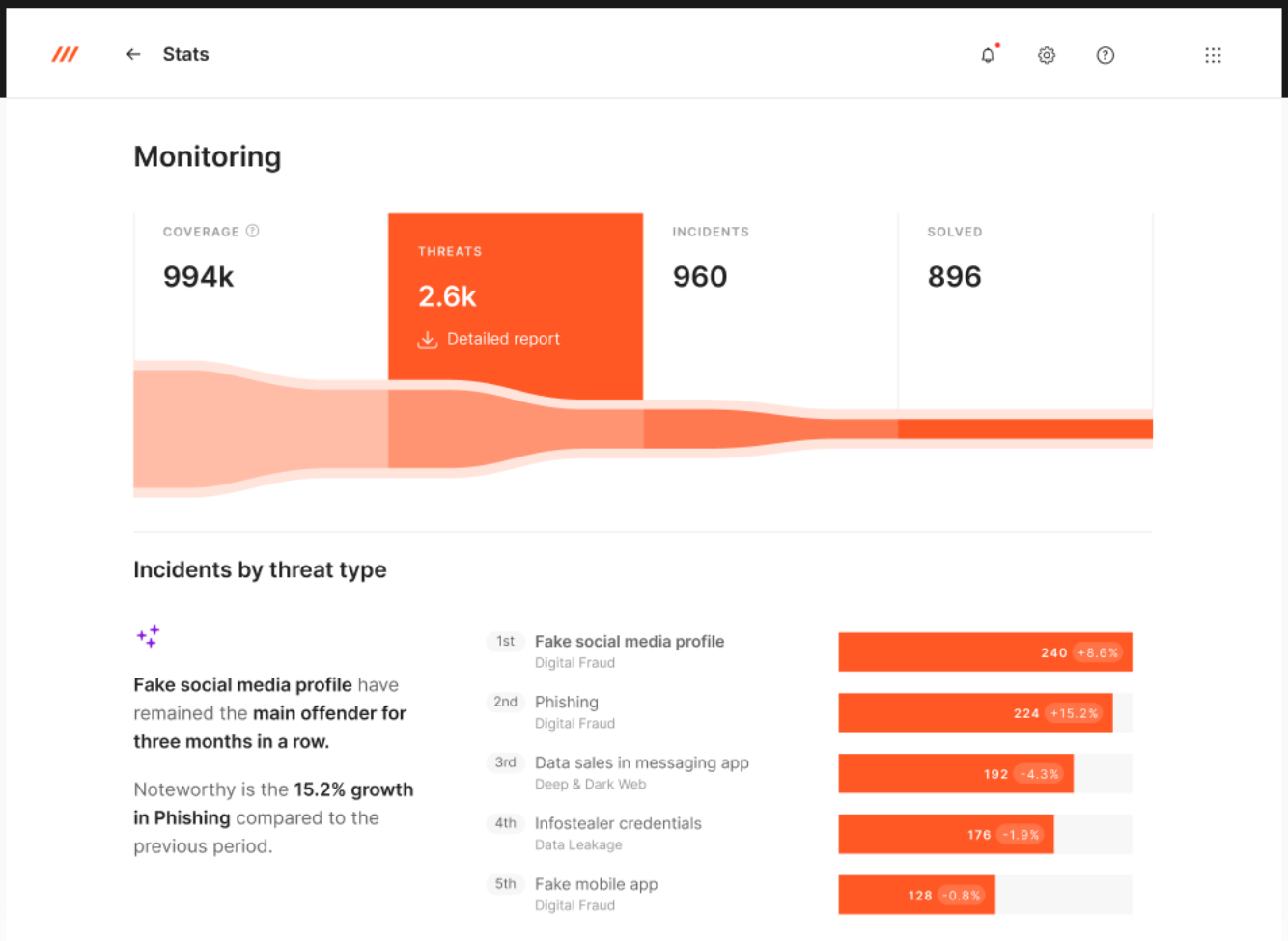
AXUR

External Cybersecurity

Axur Takes on the Heavy Lifting Against External Threats so You Can Be the Strategic Asset Your Company Calls For



With cyber-attacks increasing by 75%, you need an advanced external cybersecurity platform that stands out by offering rapid threat identification and neutralization, industry-leading takedown workflows, and comprehensive fraud intelligence, equipping businesses to counteract evolving digital threats in the landscape and making the most out of your cybersecurity budget.

- Powered by AI inspection
- Takedown with automated flows
- Minimizes the attack window

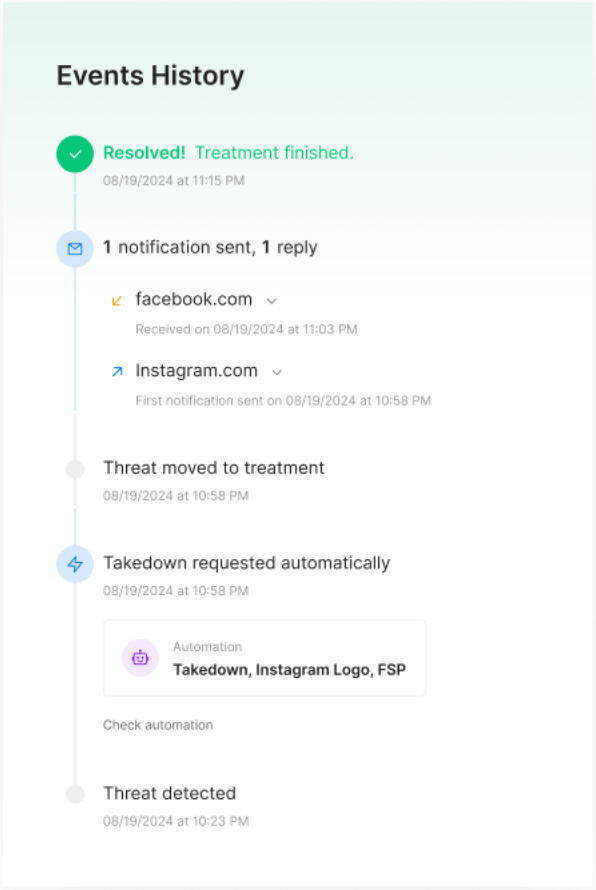
AI-powered inspection is a game-changer against cybercrime

Scale the analysis of massive signals, scouring for key attributes to categorize, prioritize, and autonomously address detections, whether to dismiss false positives or manage genuine incidents.

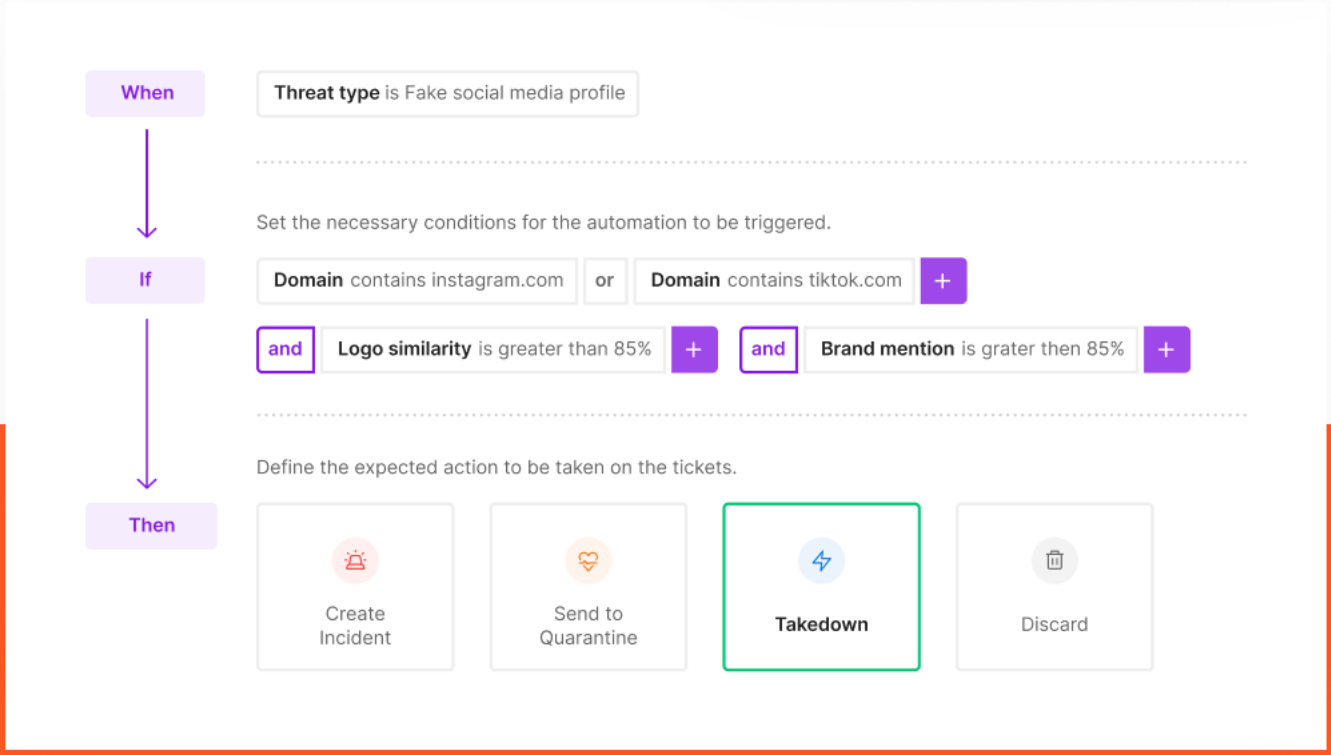
Some inspected attributes that exponentially enhance your threat management performance include:

- **89** Risk score
- Brand logo similarity
- Content language
- Brand name disambiguation
- VIP facial recognition
- Presence of password fields
- and several more!

Over 86% of Axur's detections are managed with no human touch



Real example of results from a company in the Finance sector



Automation Rulesets

Configure automated workflows to wield an unparalleled arsenal operating 24×7 for your organization, pinpointing risks and initiating auto-takedowns. Rest assured, knowing that threats are immediately addressed whenever your specified conditions are met.

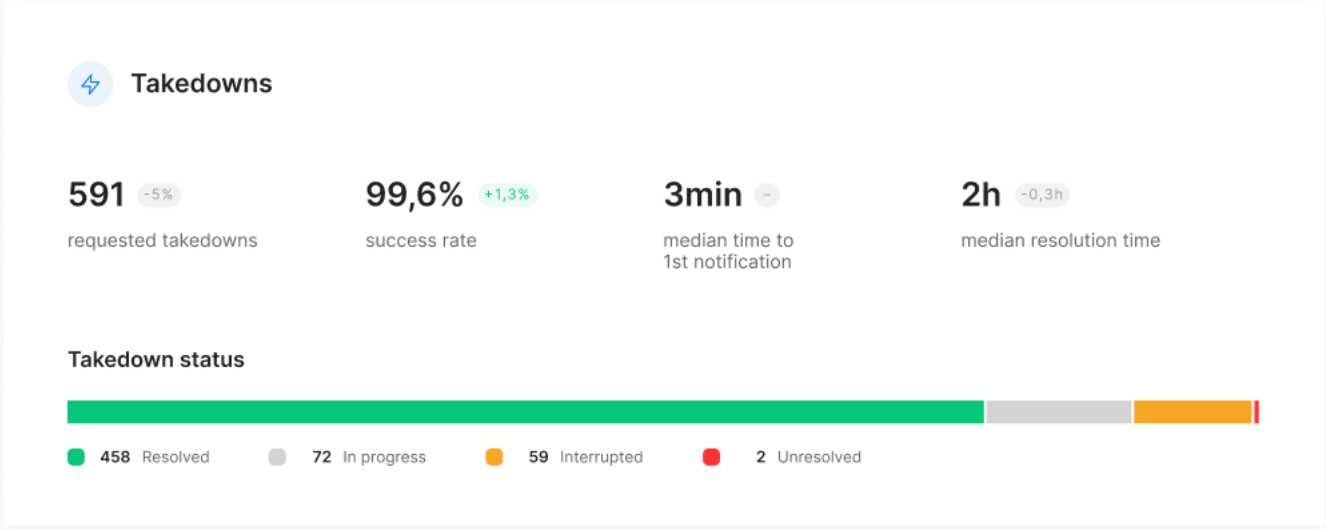
///AXUR

The gold standard for Takedown: unparalleled efficiency

5 minutes
Median time for the first notification

98.9% success rate
Free new takedown if content reappears within 15 days

9 hours of uptime
Median time for content removal



Real example of results from a company in the Retail and E-commerce sector over a period of 1 month

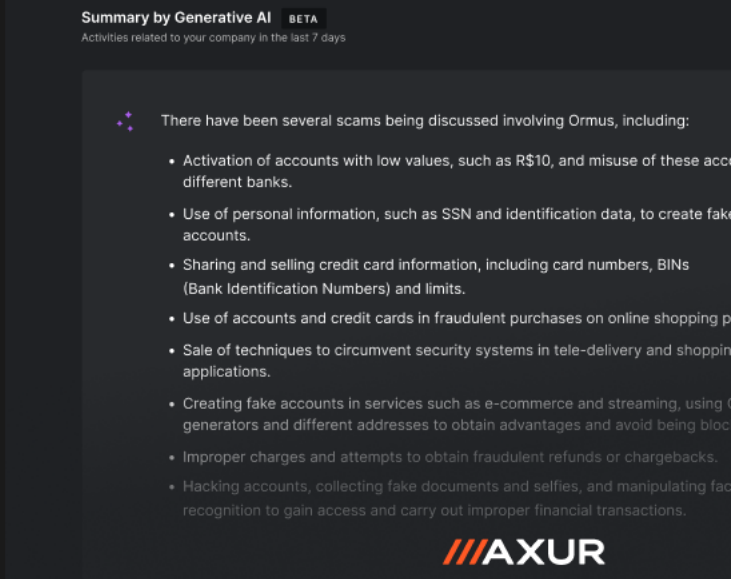
Automated takedowns, because you can't wait for human action when you need faster responses to remediate the problem.

Dramatically reduce the Mean Time to Contain (MTTC), automating the part of the process that you can control with the fastest and most accurate notifications on the market. Optimize provider analysis with orchestrated notifications for the best path and message, developed with years of experience - and constantly improving.
If the notified entity delays the response, new flows are automatically triggered to accelerate the Takedown by another route. All of this enables the scaling of takedowns unlimitedly.

Fraud intelligence to protect your business

Start your day with DeepChat, our AI generative model that provides a briefing on the most relevant Deep & Dark Web mentions to your brand, offering pinpoint insights for optimized threat management. Enhance your security with real-time anomaly alerts, including above-normal brand mentions and specific keyword tracking, ensuring prompt attention to potential threats like planned attacks or bug exploitation.

- Generative AI summary
- Anomaly alerts
- Threat Actor Profile



Advanced solutions to protect your business in the digital world

Digital Fraud

Monitor and detect content that impersonates your brand, with 24/7 coverage. Use the world's most efficient Takedown to remove external risk vectors automatically.

- Phishing
- Fraudulent brand use
- Malware
- Fake social media profile
- Fake mobile app
- Similar domain name
- Brand use in paid search

Data Leakage

Detect data exposure in real time to protect your attack surface and mitigate risks.

- Infostealer credentials
- Credit card exposure - for applications
- Credit card exposure - for issuers
- Corporate credential exposure
- Other sensitive data
- Code secret exposure
- Database exposure

Online Piracy

Reclaim your revenue that is being lost in piracy and irregular sales.

- Counterfeit or irregular sale
- Content piracy

Deep & Dark Web

Monitor threats and detect mentions of your business in Deep & Dark Web channels and groups. Track brand mentions, keywords, and multimedia content.

- Anomaly alerts
- Search for any term across thousands of channels and groups using Explore

Executives & VIPs

Monitor the data exposure of the most sensitive accounts in your company and reduce the risk of spear phishing, ransomware, and attacks using Social Engineering.

- Fake social media profile
- Exposure of personal information, credentials, phones, or credit cards

Threat Hunting

★ Latest release

Enhance your threat investigations by leveraging one of the world's largest threat databases to deeply analyze and uncover suspicious activities.

- Search Axur's extensive database with more than 23 billion credentials, as well as URLs and domains
- Learn from past incidents to prevent future attacks and build a more resilient security strategy

Security Rating

Evaluate and strengthen your security posture by eliminating external and third-party risks.

Book Your Custom Demo Now

GET A DEMO

Top global corporations

Domino's · Carrefour · Grupo Salinas · GERDAU CORSA · HAITONG · TOYOTA · natura

Discover all our solutions at axur.com

bsi ISO/IEC 27001 Information Security Management CERTIFIED

///AXUR