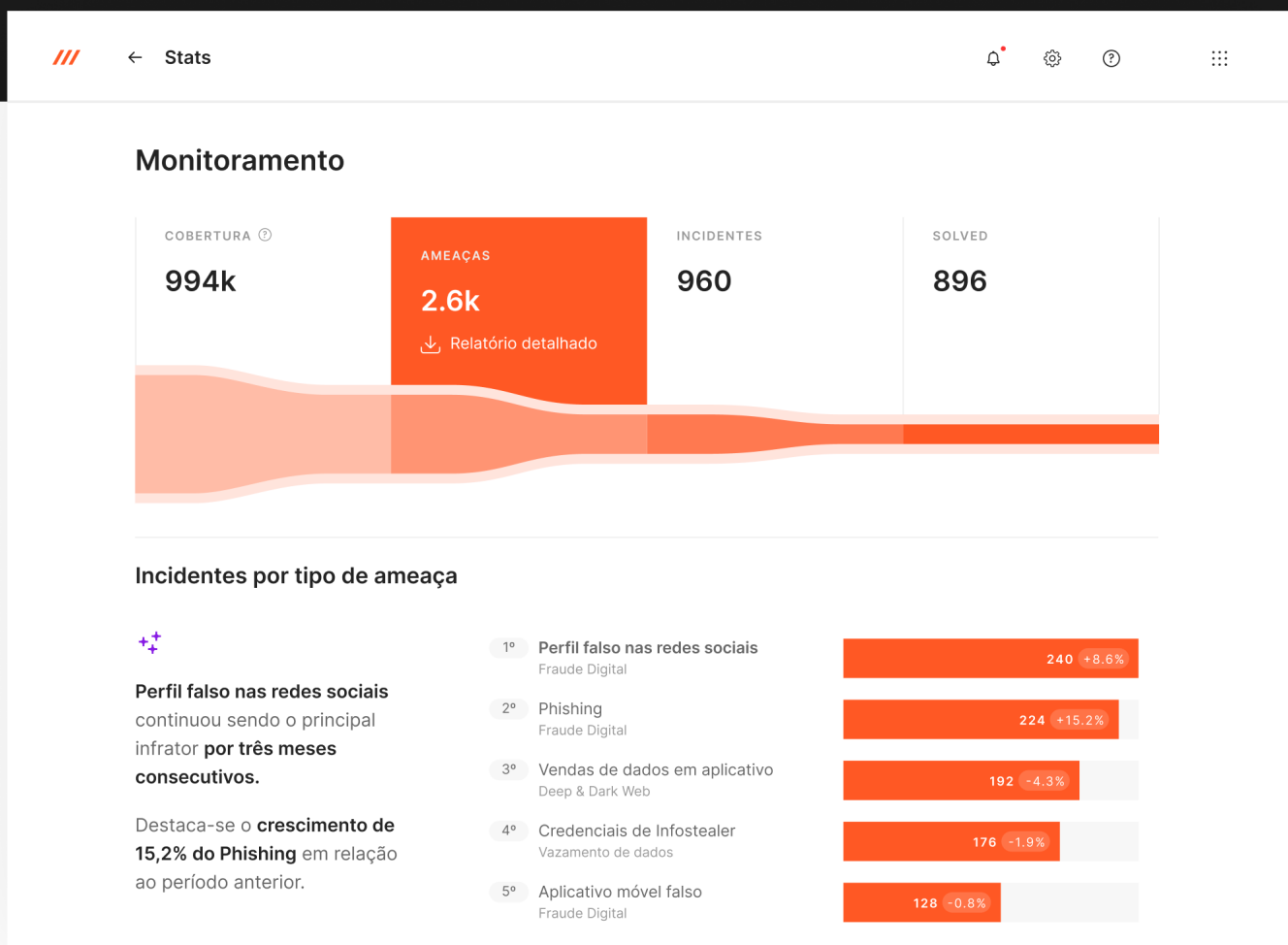


A Axur assume o trabalho pesado contra ameaças externas para que você seja o ativo estratégico da sua empresa



Com os ataques cibernéticos aumentando 75% nos últimos anos, você precisa de uma plataforma de cibersegurança externa que ofereça rápida detecção e neutralização de ameaças, fluxos automatizados de takedown e inteligência que escala para tratar ameaças cibernéticas em crescente evolução com a tecnologia mais avançada do mercado.

Inspeção impulsionada por IA

Takedown com fluxos automatizados

Minimize a janela de ataque

# A inspeção potencializada por IA é uma virada de jogo contra o cibercrime

A plataforma Axur analisa uma vasta quantidade de sinais e identifica atributos-chave para categorizar, priorizar e tratar automaticamente as detecções, seja para descartar falsos positivos ou gerenciar incidentes genuínos.

Alguns atributos inspecionados que aumentam exponencialmente o desempenho na inspeção de ameaças incluem:

- 89 Grau de risco
- Semelhança do logotipo
- Idioma do conteúdo
- Contém menção à marca
- Reconhecimento facial VIP
- Contém campo de senha
- Número de seguidores
- e muito mais!

Mais de 86% das detecções da Axur são gerenciadas sem toque humano

## Histórico de eventos

- Resolvido! Takedown finalizado.**  
02/03/2024 às 23h15
- 1 notificação enviada, 1 resposta
  - facebook.com  
Recebido em 02/03/2024 às 23h14
  - Instagram.com  
Primeira notificação enviada em 02/03/2024 às 22h59
- Ameaça movida para tratamento  
02/03/2024 às 22h58
- Takedown solicitado automaticamente  
02/03/2024 às 22h58
  - Regra de automação: Takedown, Instagram Logo, FSP
  - Ir para Automações
- Ameaça detectada  
02/03/2024 às 22h50

Exemplo real de resultados de uma empresa do setor financeiro.

Quando

Tipo de ameaça é um perfil falso em rede social



Se

Domínio contém instagram.com ou Domínio contém tiktok.com

and Semelhança do logotipo é superior a 85% e Menção da marca é maior que 85%

Então

Defina a ação esperada que deve acontecer com o ticket.

- Criar Incidente
- Enviar para Quarentena
- Takedown**
- Descartar

## Fluxos automatizados

Configure fluxos de trabalho automatizados para ter um arsenal imbatível operando 24x7 para a sua organização, identificando riscos e iniciando takedowns automáticos. Fique tranquilo, sabendo que as ameaças são imediatamente tratadas sempre que as condições especificadas forem atendidas.

# O padrão ouro em Takedown: com eficiência imbatível



**5 minutos**  
Mediana para a primeira notificação



**98.9% de sucesso**  
Nova remoção grátis caso o conteúdo volte em 15 dias



**9 horas de uptime**  
Mediana para remoção de conteúdo



Exemplo real de resultados de uma empresa do setor de Varejo/E-commerce ao longo de um período de 1 mês.

**Takedowns automáticos, porque você não precisa esperar por uma ação humana para remediar o problema.**

Reduza drasticamente o Tempo Médio para Contenção (MTTC), automatizando a parte do processo que você pode controlar com as notificações mais rápidas e assertivas do mercado. Otimize a análise do provedor com notificações orquestradas para o melhor caminho e mensagem, desenvolvidas com anos de experiência - e em constante aprimoramento. Se a entidade atrasar a resposta, novos fluxos são automaticamente acionados para acelerar o Takedown por outra rota. Tudo isso permite a escalabilidade das remoções de forma ilimitada.

## Inteligência que escala para ficar protegido

Comece o seu dia com o DeepChat, nossa IA generativa que sumariza as menções mais relevantes à sua marca na Deep & Dark Web, oferecendo insights precisos para uma gestão de ameaças otimizada. Fique tranquilo configurando alertas de anomalias, incluindo menções acima do normal e rastreamento específico de palavras-chave, garantindo atenção imediata a potenciais ameaças como ataques planejados ou exploração de vulnerabilidades, em tempo real.

- Resumo com IA Generativa
- Alertas de anomalias
- Perfil do Threat Actor

Resumo por IA generativa BETA  
Atividades relacionadas a sua empresa nos últimos 7 dias

- Houve várias fraudes sendo discutidas envolvendo Ormus, incluindo:
- Ativação de contas com valores baixos, como R\$ 10, e uso indevido dessas contas em diferentes bancos.
  - Uso de informações pessoais, como CPF e dados de identificação, para criar contas falsas.
  - Compartilhamento e venda de informações de cartões de crédito, incluindo número de cartão, BINs (Bank Identification Numbers) e limites.
  - Uso de contas e cartões de crédito em compras fraudulentas em plataformas de compras online.
  - Venda de técnicas para burlar sistemas de segurança em aplicativos de tele-entrega de compras.
  - Criação de contas falsas em serviços como e-commerce e streaming, usando dados de CPF e endereços diferentes para obter vantagens e evitar bloqueios.
  - Cobranças indevidas e tentativas de obter reembolsos ou estornos fraudulentos.
  - Invasão de contas, coleta de documentos e selfies falsos, e manipulação do reconhecimento facial para obter acesso e realizar transações financeiras indevidas.

**AXUR**

Última atualização em 12/09/2023

# Soluções avançadas para **proteger** seu **negócio** no mundo digital

## Fraude digital

Monitore conteúdos que se passam por sua organização, com cobertura 24/7. Utilize o Takedown mais eficiente do mundo para eliminar automaticamente vetores de risco externos.

- Phishing
- Uso fraudulento de marca
- Malware
- Perfil falso em rede social
- App mobile falso
- Nome de domínio similar
- Uso de marca em busca paga

## Vazamento de dados

Detecte exposições de dados em tempo real para proteger sua superfície de ataque e mitigar riscos.

- Credencial de infostealer
- Exposição de cartão de crédito - para aplicações
- Exposição de cartão de crédito - para emissões
- Exposição de credencial corporativa
- Outros dados sensíveis
- Exposição de segredo de código
- Exposição de base de dados

## Pirataria Online

Recupere sua receita que está sendo perdida em pirataria e vendas irregulares.

- Pirataria ou venda irregular
- Pirataria de conteúdo

## Deep & Dark Web

Monitore ameaças e detecte menções ao seu negócio em canais e grupos da Deep & Dark Web. Rastreie menções à marca, palavras-chave e conteúdo multimídia.

- Pesquise qualquer termo em milhares de canais e grupos usando Explorar
- Alertas de anomalia

## Executivos & VIPs

Monitore a exposição de dados das contas mais sensíveis da sua empresa e reduza o risco de spear phishing, ransomware e ataques que utilizam engenharia social.

- Perfil falso em rede social
- Exposição de informações pessoais, credenciais, telefones ou cartões de crédito

## Threat Hunting

★ Último lançamento

Aprimore suas investigações de ameaças aproveitando um dos maiores bancos de dados de ameaças do mundo para analisar profundamente e descobrir atividades suspeitas.

- Pesquise no extenso banco de dados da Axur com mais de 23 bilhões de credenciais, bem como URLs e domínios
- Aprenda com incidentes passados para prevenir ataques futuros e construir uma estratégia de segurança mais resiliente

## Avaliação de segurança

Avalie e fortaleça sua postura de segurança eliminando riscos externos e de terceiros.

Agende **uma demo** agora

Top global corporations



AGENDE UMA DEMO

Conheça todas as nossas soluções: [axur.com](https://axur.com)

