///AXUR

Vazamento de Dados

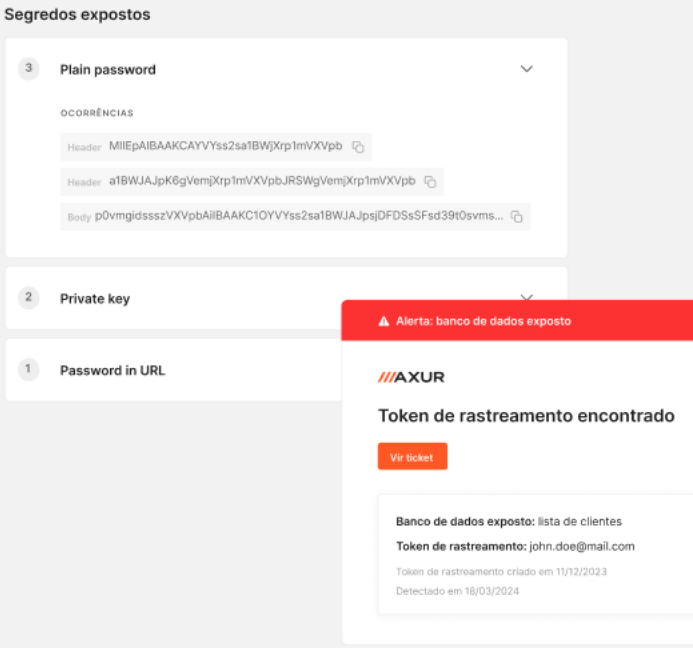
Seja alertado de exposição de dados e proteja sua superfície de ataque externa

Problema

Threat actors exploram violações de dados e se utilizam disso para golpes e ciberataques. Mais de 81% dos ataques de ransomware têm origem em credenciais corporativas expostas. Você precisa de ajuda para proteger as informações mais valiosas de sua organização e preservar o acesso privilegiado com uma plataforma proativa que monitore e detecte continuamente possíveis violações e exposições em tempo real.

Solução

A Axur oferece uma resposta robusta a esse desafio, possibilitando que você garanta a segurança de seus dados sensíveis e também obtenha uma visão abrangente de sua superfície de ataque externa. Detecte credenciais de acesso, senhas comprometidas, cartões expostos, chaves de código ou arquivos e dados mais sensíveis. Além disso, nossas soluções contemplam monitoramento para credenciais de plataformas próprias, para responder prontamente e gerenciar o risco de forma eficaz.



Aprimore o tempo de resposta e mitigue impactos com leis de governança e proteção de dados

- Monitoramento diário de domínios e exposição de credenciais
- Buscas automáticas por referências a marcas, produtos, serviços e documentos confidenciais da empresa
- Detecta venda de dados em fóruns da Deep & Dark web e mercados na darknet
- Verificação regular de sites de pastes, usados para disseminar informações que possibilitam ataques
- Processamento de grandes vazamentos

+42 bilhões de credenciais

detectadas em vazamentos de dados

1 bilhão adicionadas mensalmente

Exposição de credencial corporativa

Monitore a exposição de credenciais corporativas usadas por seus funcionários em ambientes e aplicativos. Acesse um registro histórico de credenciais expostas para tomar decisões rápidas, responder prontamente e mitigar riscos.

Credencial de infostealer

Esteja ciente das credenciais comprometidas de clientes e funcionários detectadas em malwares como infostealers. O monitoramento direcionado da Axur de domínios e URLs determina com precisão quais credenciais autenticam com sucesso em sites ou aplicativos específicos.

- Identifique ataques complexos que podem burlar a MFA;
- Detecção contextual de todos os dados e informações expostos da máquina infectada.

Exposição de credencial de cliente

Detecte credenciais expostas usadas para fazer login em sua plataforma web, site de comércio eletrônico ou ambiente digital. Responda rapidamente exigindo uma redefinição de senha ou restringindo transações e atividades.

- Limpeza inicial do banco de dados
- Alertas via Webhook

Fontes monitoradas para exposição de credenciais:

- Deep & Dark Web, incluindo grupos, fóruns e comunidades no Telegram/WhatsApp/Discord
- Logs de malware;
- Sites não catalogados ou não indexados;
- Darknets (como TOR, Freenet, I2P, Usenet);
- Canais de Internet Relay Chat (IRC);
- Fóruns abertos e fechados na web;
- Grandes vazamentos (Canva, Trello, etc.).

Sites de paste, incluindo:

Pastebin | Ghostbin | Bitbin | Openstack | ControlC
Dpaste | Hastebin | Paste2 | Pasteorg | Zeropaste

Exposição de cartão para aplicações

Use uma API para obter acesso instantâneo a um vasto banco de dados de cartões expostos. Valide a segurança de um cartão antes de qualquer aprovação de compra ou registro em sua plataforma, minimizando o risco de transações indevidas.

- Integração perfeita com sistemas internos e outras aplicações
- Uma lista global de cartões expostos para referência
- Recursos de IA para identificação automática de cartões expostos.

Exposição de cartão para emissores

Monitore os BINs de seus cartões de crédito em busca de vazamentos na Surface e na Deep & Dark Web.

- API avançada e notificações por webhook;
- Detalhes como número do cartão, CVV, data de validade, data de detecção e a fonte do vazamento.

Exposição de base de dados

Insira tokens disfarçados como dados reais em seus bancos de dados e seja alertado se eles forem encontrados em qualquer vazamento. Os Tokens de Rastreamento simplificam o processo de resposta e auditoria de vazamentos para minimizar as consequências legais.

- Ajuda a confirmar a legitimidade do banco de dados e controlar o acesso ao longo do tempo;
- Isola a fonte de dados expostos por meio de tokens exclusivos para bancos de dados compartilhados com terceiros.

Exposição de segredo de código

Identifique chaves de código de seus domínios, como tokens, senhas e arquivos de configuração críticos que podem estar expostos em códigos ou commits públicos no GitHub.

Outros dados sensíveis

Identifique a exposição de dados pessoais, proprietários ou sensíveis associados à sua marca em várias plataformas e arquivos, como Scribd, 4Shared, Trello e S3 Buckets hospedados na Amazon AWS, Azure Blobs e Digital Ocean Spaces.

Proteja seus dados agora

Conheça todas as nossas soluções: axur.com

Agende uma demo

///AXUR