SumUp reduz chargebacks e recupera mais de R$ 420 mil com monitoramento preventivo da Axur

Sobre a empresa

A SumUp é uma fintech global fundada em 2012 que oferece soluções de pagamento e serviços financeiros para pequenos e médios negócios. Com presença em 34 países, atende mais de 3,5 milhões de clientes, democratizando o acesso a tecnologias de pagamento e impulsionando o empreendedorismo.

Problema

Em 2020, cibercriminosos estavam conseguindo aplicar muitos golpes de checkers, fraudes que usam geradores de CPF para criar cadastros falsos. Os fraudadores se organizavam em grupos e fóruns da Deep & Dark Web para compartilhar técnicas, trocar informações sobre vulnerabilidades e coordenar ataques contra clientes da SumUp. Sem visibilidade sobre essas conversas, a empresa reagia aos golpes apenas depois que os chargebacks já haviam ocorrido.

Solução

A Axur se tornou uma aliada estratégica para recuperar o controle sobre as fraudes que já impactavam a operação.

Com o monitoramento contínuo de grupos e fóruns onde fraudadores se organizavam, a SumUp conseguiu mapear os esquemas, entender os modus operandi e bloquear novas tentativas antes que resultassem em chargebacks.

Impacto na operação

Mais de R$ 420 mil recuperados em apenas 6 meses

ROI positivo para a empresa

Redução drástica de golpes com checkers e cadastros falsos

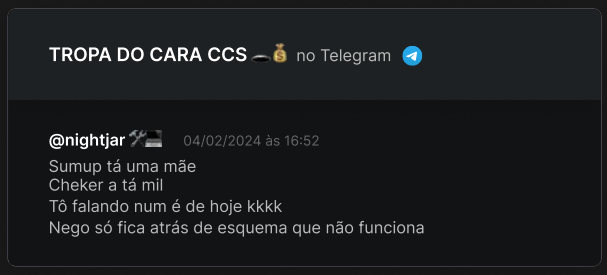

Imagem 1: Prints de golpista falando sobre a SumUp antes da parceria com a Axur

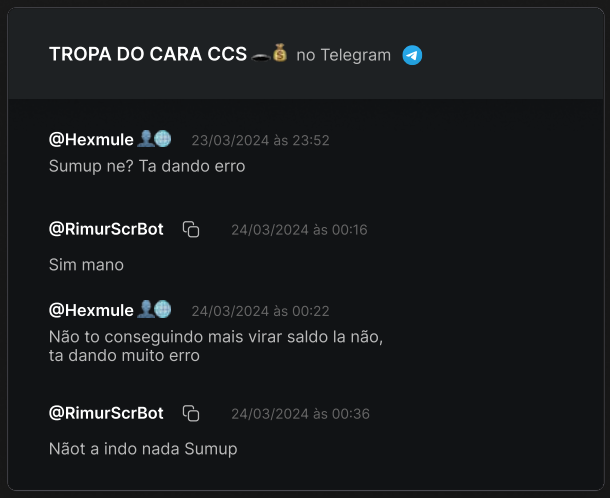

Imagem 2: Prints de golpistas reclamando que estava impossível aplicar golpes na SumUp após a parceria com a Axur

Soluções para detectar ameaças na Deep & Dark Web

Antecipando ameaças com inteligência cibernética

O monitoramento preventivo da Deep & Dark Web permite interceptar conversas e identificar esquemas em andamento. A plataforma da Axur rastreia menções à marca, discussões sobre vulnerabilidades, compartilhamento de dados de clientes e até a comercialização de credenciais comprometidas.

Essa abordagem preventiva substitui o modelo reativo tradicional, onde as ameaças só são descobertas depois que os chargebacks já foram solicitados e os prejuízos financeiros já ocorreram.

Detecção multimídia com visão computacional

Os fraudadores não se limitam a texto. Muitas vezes, compartilham prints de tela, vídeos tutoriais e imagens com instruções de como aplicar golpes.

A tecnologia de Visão Computacional da Axur (Clair) analisa automaticamente áudios, vídeos e imagens compartilhados na Deep & Dark Web, transcrevendo e identificando menções à marca mesmo quando o nome aparece apenas em formato visual.

Exploração e alertas customizados

A plataforma permite que equipes de segurança pesquisem e explorem ativamente qualquer termo relacionado à sua operação em um ambiente seguro. Além disso, alertas customizados notificam a equipe imediatamente quando uma nova ameaça é detectada, permitindo resposta rápida e coordenada.

A Axur também oferece suporte especializado para investigar esquemas mais complexos, fornecendo contexto completo sobre perfis de fraudadores, suas táticas e motivações.

Impacto no combate a fraudes

As soluções da Axur ajudam empresas a recuperar o controle da marca, trazendo retorno financeiro direto e tornando-se fundamentais para o combate de fraudes, especialmente em períodos de lançamento de novos produtos.

Descubra como proteger sua empresa das ameaças da Deep & Dark Web

AGENDE UMA DEMO

Gartner Peer Insights 4.9

Conheça todas as nossas soluções: **axur.com**

///AXUR