

[Sobre la empresa](#)

SumUp reduce los chargebacks y recupera más de R\$ 420 mil con el monitoreo preventivo de Axur

⌚ Problema

En 2020, los ciberdelincuentes lograban ejecutar numerosos fraudes tipo checkers, ataques que utilizan generadores de CURP para crear registros falsos. Los estafadores se organizaban en grupos y foros de la Deep & Dark Web para compartir técnicas, intercambiar información sobre vulnerabilidades y coordinar ataques contra clientes de SumUp. Sin visibilidad sobre estas conversaciones, la empresa solo podía reaccionar ante los incidentes después de que los chargebacks ya se habían producido.

Impacto en la operación



Más de R\$ 420 mil recuperados en solo 6 meses



ROI positivo para la empresa



Reducción drástica de fraudes con checkers y registros falsos



SumUp es una fintech global fundada en 2012 que ofrece soluciones de pago y servicios financieros para pequeñas y medianas empresas. Con presencia en 34 países, atiende a más de 3,5 millones de clientes, democratizando el acceso a tecnologías de pago e impulsando el emprendimiento.

💡 Solución

Axur se convirtió en un aliado estratégico para ayudar a recuperar el control de los fraudes que ya afectaban la operación.

Gracias al monitoreo continuo de grupos y foros donde se organizaban los estafadores, SumUp pudo mapear los esquemas, comprender los modus operandi y bloquear nuevos intentos antes de que se convirtieran en chargebacks.

TROPA DO CARA CCS 💰 en Telegram

@nightjar 🎨 02/04/2024 a las 16:52

SumUp está re fácil 😊

El checker anda a full 🔥

Se lo digo, esto no es de hoy jajaja

La banda nomás anda buscando esquemas que ni sirven

Imagen 1: Capturas de pantalla de estafadores hablando sobre SumUp antes de la alianza con Axur

TROPA DO CARA CCS 💰 en Telegram

@Hexmule 🤖 23/03/2024 a las 23:52

¿SumUp, no? Está tirando error

@RimurScrBot 📁 24/03/2024 a las 00:16

Sí, bro

@Hexmule 🤖 24/03/2024 a las 00:22

Ya no puedo "convertir" saldo ahí, no...
está tirando un montón de errores

@RimurScrBot 📁 24/03/2024 a las 00:36

No está jalando nada en SumUp

Imagen 2: Estafadores quejándose de que era prácticamente imposible cometer fraudes en SumUp después de la alianza con Axur

Soluciones para detectar amenazas en la Deep & Dark Web



Anticipación de amenazas con inteligencia cibernetica

El monitoreo preventivo de la Deep & Dark Web permite interceptar conversaciones e identificar esquemas en curso. La plataforma de Axur rastrea menciones a la marca, discusiones sobre vulnerabilidades, el intercambio de datos de clientes e incluso la comercialización de credenciales comprometidas. Este enfoque preventivo reemplaza el modelo reactivo tradicional, en el que las amenazas solo se detectan después de que los chargebacks ya fueron solicitados y las pérdidas financieras ya ocurrieron.



Exploración y alertas personalizadas

La plataforma permite que los equipos de seguridad investiguen y exploren activamente cualquier término relacionado con su operación en un entorno seguro. Además, las alertas personalizadas notifican al equipo de inmediato cuando se detecta una nueva amenaza, habilitando una respuesta rápida y coordinada.



Detección multimedia con visión computacional

Los estafadores no se limitan al texto. Con frecuencia comparten capturas de pantalla, videos tutoriales e imágenes con instrucciones sobre cómo ejecutar fraudes.

La tecnología de Visión Computacional de Axur (Clair) analiza automáticamente audios, videos e imágenes compartidos en la Deep & Dark Web, transcribiendo e identificando menciones a la marca incluso cuando el nombre aparece únicamente en formato visual.



Impacto en la lucha contra el fraude

Las soluciones de Axur ayudan a las empresas a recuperar el control sobre su marca, generando un retorno financiero directo y convirtiéndose en un pilar clave para el combate contra el fraude, especialmente durante períodos de lanzamiento de nuevos productos.



Descubra cómo proteger a su empresa de las amenazas de la Deep & Dark Web

[AGENDE UNA DEMO](#)

Gartner
Peer Insights