Major Brazilian Retailer Automates Protection for Over 50 Million Customers with Axur

About the Company

One of Brazil's largest online retailers, with more than 50 million registered customers. The company operates nationwide and faces challenges typical of high-volume e-commerce operations, especially during peak events such as Black Friday.

Problem

Attackers could use compromised accounts—without the victims' consent—to access data, test stolen credit cards, or carry out activities that degrade the user experience. Leveraging an existing compromised account is easier than creating a new one with stolen data. Manual analysis had become repetitive and costly, particularly during critical periods like Black Friday, when speed is essential.

Solution

The security team implemented an automation that queries breach intelligence through Axur's API, leveraging platform-configured filters to retrieve only relevant credentials.

A custom script acts as a bridge between the Axur Platform and internal systems, transparently resetting passwords without disrupting the user experience.

Operational Impact

Over 1,500 accounts remediated automatically since implementation

Complete elimination of the manual remediation queue

100% of leaked credentials reset automatically

Black Friday 2022 marked as a milestone for successful implementation

"Thanks to Axur's development team, we can consume data via the API and fully automate this process. Today, essentially every leaked credential is reset, and we're confident it won't be used fraudulently."

Security Analyst
Major Brazilian Retailer

The Scale Challenge During Peak Periods

Before automation, analysts manually transferred data from the Axur Platform to internal systems. As Black Friday 2022 approached, it became clear this model would not scale to meet the surge in demand during one of the most critical periods in Brazilian e-commerce.

Although credential compromise occurs outside the company's perimeter, its impact is felt directly by the retailer—affecting user experience and driving additional costs related to customer support, account recovery, and fraud prevention.

Continuously Evolving Automation

Early versions of the automation still required analyst intervention to adapt incoming data. With each iteration, the process became more efficient, reducing operational effort while keeping pace with increasing incident volumes.

By adopting Axur's API and advanced filtering, the workflow evolved to ingest only relevant credentials and ultimately became fully automated—consuming, preparing, and processing data end to end with no human intervention.

Transparent and Proactive Protection

Incident response is transparent to users, who are prompted to change their passwords only when performing sensitive actions, such as completing a purchase. This approach reduces friction and preserves the customer experience during browsing.

By accelerating incident remediation, the automation significantly shortens the exposure window for leaked credentials, invalidating them before they can be exploited in malicious activity.

Integration That Amplifies Results

The retailer already had mature internal processes and APIs capable of supporting automation at this scale. The security team identified that creating a script to connect the Axur Platform to existing internal systems was sufficient.

By monitoring external environments—including the Deep and Dark Web—the Axur Platform delivers filtered, high-confidence alerts, providing early visibility into data leaks and enabling fast, accurate, and scalable response.